

The APV Guideline
”Computerized Systems”
based on Annex 11 of the EU-GMP Guideline

Contributed by the APV Specialist Section „Information Technology“

The comments in this paper reflect the
personal views of the members of the APV Specialist Section

Foreword

The Regulations for Pharmaceutical Manufacturers dated from August 1994 created the legal basis for the general implementation of the EU-GMP Guideline with its Annex 11 "Computerized Systems".

This Annex describes the requirements for using computerized systems in the GMP sector. In addition, this Annex is also applicable to the data entry part of the GCP area as described in the EU-GCP Guideline.

The brevity of the sections in Annex 11 leaves much room for interpretation, creating considerable uncertainty among the manufacturers and users of computerized systems.

That is why the members of the APV Specialist Section „Information Technology“ has interpreted Annex 11 on the basis of previous guidelines, publications and their own experience. Their comments are published below as an APV Guideline.

Please note that this APV-Guideline represents but *one* procedure to develop and operate computerized systems. It is therefore the responsibility of the Pharmaceutical Manufacturer to determine priorities and to reduce or increase the stringency of the applicable procedures on the basis of his own defined criteria.

The following members of the APV Specialist Section „Information Technology“ worked on this APV Guideline:

Dr. Helmut Bender	Boehringer Ingelheim KG
Dr. Rango Dietrich	Byk Gulden GmbH
Dr. Heinrich Hambloch	GITP (Head of the Specialist Section)
Mr. Ottomar Henning	Schering AG
Mr. Karl-Heinz Menges	State Govt. Headquarters Darmstadt
Dr. Dirk Spingat	Bayer AG

Notes

- In order to distinguish between Annex 11 and this guideline, the areas covered by Annex 11 are referred to as "points" and allocation within the bounds of this guideline as "sections". The guideline deals with all points in Annex 11 but does not retain the same order in favour of a more rational structure:

Sections in the APV comments	Points in Annex 11
General part	definitions, principles, points 1, 18
Life-cycle model	points 2, 3, 4, 5, 7, 11
Access authorization	points 8, 10
Data input	points 6, 9, 19
Data storage and backup	points 12, 13, 14
Error handling and system failure	points 15, 16, 17

- The numbers in the right margin refer to the points and sentences in Annex 11 ([8.3] means point 8, sentence 3: In a process ... should ...). The text of Annex 11, numbered accordingly, can be seen in Appendix 7.1.
- Terms set in *italics* are explained at length in the glossary
- The comments presuppose that all activities and evaluations listed are reproducibly documented on a suitable medium even if this is not stated explicitly in the respective text.

Contents

1 GENERAL	5
1.1 Definitions	5
1.2 Principles	6
1.3 Personnel	7
1.4 Third-party services	8
2 LIFE-CYCLE MODEL	9
2.1 Phase-related activities	10
2.2 Cross-phase activities	14
2.3 Prospective and retrospective validation	16
3 ACCESS AUTHORIZATION	17
4 DATA INPUT	18
5 DATA STORAGE AND BACKUP	19
6 ERROR HANDLING AND SYSTEM FAILURE	20
7 ANNEX	21
7.1 Supplementary guideline for computerized systems: Annex 11	21
7.2 Glossary	24
7.3 References	25

1 General

1.1 Definitions

System, computerized system

If the term "system" is applied to computerized systems (CS), these should include the combination of all hardware and software elements. The activities and techniques involved in creating and operating a CS are defined and implemented in the life-cycle model (see section 2). [0.1]
[0.2]

Reflecting this general approach, peripheral components required for input such as the following are part of the system. [2.2]
[4.1]

- barcode reader
- scanner
- on-line data collection from processes
- manual collection of data via keyboard

Electronic processing embraces the following system components, and all combinations of these: [4.1]

- Computer hardware (CPU, network components)
- system-specific software components such as
 - ◆ operating systems
 - ◆ network software
 - ◆ database environments
 - ◆ drivers for peripheral devices
 - ◆ programming languages (interpreters, compilers)
 - ◆ PLC development environments
- Application programs such as
 - ◆ word processors
 - ◆ databases
 - ◆ spreadsheets
 - ◆ graphics programs
 - ◆ materials management programs
 - ◆ production planning systems
 - ◆ PLC programs and process control systems

Output requires the relevant system parts of the components to be processed and peripheral hardware such as

- display screens
 - printers
 - media (paper)
 - data storage media
 - controls
- [4.1]

1.2 Principles

All CS that require validation should be identified. This includes all CS that can affect the product quality and quality assurance in the areas mentioned in the Annex, that is manufacture, warehousing, distribution and quality control.	[0.3]
For this purpose there should be specifications for the identification of such CS together with decision-making criteria for classification as "requiring validation" .	[0.4]
For CS, the Annex requires that general GMP principles be considered and even goes beyond the classical scope of GMP in that the distribution of medicines is also covered by this Annex.	[0.3]

1.3 Personnel

There should be sufficient, qualified staff with the relevant experience to carry out tasks for which the Pharmaceutical Manufacturer is responsible in connection with the planning, introduction, application (operation), application consultancy on, and regular monitoring of, computerized systems. [1.1]
[1.2]
[1.3]

Staff qualifications should be assessed on the basis of professional training, education and experience in handling and developing computerized systems. Qualification requirements should be determined by the field of work in which the staff will be operating. Staff should only be deployed in areas suited to their skills and training.

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

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 CS.

The Pharmaceutical Manufacturer is responsible for ensuring all staff who have to perform tasks in connection with computerized systems are given the requisite training and for familiarizing them with the relevant guidelines on computerized systems. That should also apply to system developers, maintenance and repair staff and staff whose work could affect the documented operability of the systems. [0.5]

Apart from a basic training in computerized systems, newly recruited staff should also be trained in the tasks assigned to them personally. Furthermore, continuous training should also be ensured according to standard training programs and implementation in practice should be assessed from time to time.

In connection with training, the GMP 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.

1.4 **Third-party services**

Where external companies are involved in the operation or development of computerized systems, the responsibilities should be defined precisely in appropriate written agreements as specified for the GMP sector as contract manufacture agreements.

[18.1]
[5.2]

Technical aspects or those concerning quality assurance included in the agreement should be formulated together with competent persons qualified in pharmaceutical technology, analytics and the development, maintenance, operation and application of computerized systems.

The external company should not sub-contract any work which it has accepted contractually without the written approval of the contracting party.

Even where tasks are partly contracted out to external companies the Pharmaceutical Manufacturer continues to hold responsibility for the suitability and operability of the computerized systems.

The Pharmaceutical Manufacturer is responsible for assessing whether or not the external company is sufficiently competent to carry out the required tasks successfully. He should check this, where necessary, by conducting an audit and/or by obtaining appropriate documents.

The Pharmaceutical Manufacturer should check regularly that the external company is developing, maintaining or operating the computerized system properly and in accordance with the previously specified description of the system.

The external company should have suitable premises and the necessary equipment, sufficient know-how and experience as well as competent staff to be able to perform the contracted work satisfactorily. Contract work related to computerized systems should only be accepted by external companies if it has been checked and documented that the above conditions can be met.

The contracting party should ensure that the contractor is aware of all the problems involved in the contracted work which could present a risk affecting patient safety, quality of the drugs, the space, facilities, staff or other materials and products.

Evidence of the defined staff qualifications should also be submitted even for staff at external companies; these qualifications depend on the work performed by the individual member of staff.

The contracting party should be provided with the contractually agreed life-cycle documentation during the agreed storage period (see section 2.1 - Phase-related activities "Withdrawal").

The contract should allow the contracting party to inspect the facilities and working methods of the contractor.

The contractor should be aware that the relevant authorities are authorized to inspect his facilities.

The contract should be reviewed by qualified persons on behalf of the pharmaceutical Manufacturer.

2 Life-cycle model

Computerized systems should be developed, implemented and operated in accordance with the life-cycle model which takes account of the following life-cycle phases:	[2.2] [2.3] [5.1] [5.2]
<ul style="list-style-type: none">• Creating a project outline• Creating a quality plan• Creating user requirements specifications• Creating system design specifications• Performing risk analysis• Developing system components (software and hardware)• Developing the user and the system manual• Installation and operation• Acceptance test planning and execution• Release• Operation with<ul style="list-style-type: none">◆ change control◆ system monitoring and maintenance◆ error handling◆ and all Annex-11-specific activities described in the sections 3, 4, 5 and 6.• Phase out	[7.1] [11] [15 - 17]
The following are cross-phase activities / evaluations:	
<ul style="list-style-type: none">• Planning and execution out tests• Configuration control• Planning and conducting audits• Planning and conducting <i>reviews</i>	[7.1] [4.1]
Standard operating procedures (SOPs) should be available for all life-cycle phases and all cross-phase activities; these should describe the activities in sufficient detail for specialists. The results of the activities obtained should be tested on the basis of the SOPs as part of a <i>review</i> and, if necessary, corrected until they comply. This ensures a formal quality assurance system.	
The life-cycle phases and cross-phase activities described below are recommendations. Depending on the complexity of the CS, these may be combined rationally or further subdivided by any involved party (Pharmaceutical Manufacturer, third party contractors).	[5.2]

2.1 **Phase-related activities**

- Creating a project outline [2.2]
[2.3]
The project outline describes the planned project in abridged form and includes the following details: [4.2]
[5.2]
 - ◆ aim of and reason for project
 - ◆ repercussions for other systems or operations
 - ◆ regulatory environment
 - ◆ main persons involved
 - ◆ pre evaluation of suppliers

- Creating a quality plan [2.1]
[2.2]
The quality plan should document the following evaluations and, where necessary, adjust these in line with the project (version control): [2.3]
[5.2]
 - ◆ project-specific phases of the life-cycle and cross-phase activities
 - ◆ list of the guidelines and SOPs for life-cycle activities and cross-phase activities
 - ◆ created documentation
 - ◆ list of all system components (see section 1.1 Definitions)
 - ◆ control measures and committees
 - ◆ project organization with responsibilities and schedules

- Creating user requirements specifications [2.2]
[2.3]
The user requirements specifications describe the system from the user's point of view. This should be sufficiently detailed for each system component (see section 1.1 Definitions) as to allow the system design specifications to be derived from this. [4.2]
[5.2]
The user requirements specifications should be drawn up by the users in co-operation with the IT professionals.
The user requirements specifications should form the basis for the risk analysis, the system design specifications and the acceptance test, and should be drawn up bearing this in mind.

<ul style="list-style-type: none"> • Performing risk analysis 		
<p>Risk analysis should investigate and assess the direct and indirect effects of the CS on GMP. The effects of every function laid down in the user requirements specifications should be investigated and assessed in order to guarantee perfect drugs that comply with the specifications.</p>		[2.2] [2.3] [4.2] [5.2]
<p>Furthermore, all GMP-critical data which require restricted access should be ascertained. These are data which potentially influence the quality of the drug.</p>		9.1]
<p><i>Risk analysis</i> should be taken into consideration for the following activities:</p>		
<ul style="list-style-type: none"> • creating the system design specifications • creating the test plans for the individual functions (see section 2.2 "Testing") • taking a decision on whether or not to re-validate the CS after changes 		[7.1]
		[11]
<ul style="list-style-type: none"> • Creating system design specifications 		
<p>The system design specifications should describe the system from the system developer's point of view. It should be possible to create the system exclusively using these specifications.</p> <p>The development specifications should be drawn up by IT professionals such that they can serve as a basis for the module test and the integration test. It must be possible to refer back to the user requirements specifications.</p>		[2.2] [2.3] [4.2] [5.2]
<ul style="list-style-type: none"> • Developing system components 		
<p>The system components should be developed on the basis of the system design specifications and integrated gradually into a CS. In order to ensure that all developers adopt a standard approach and thus maintenance of a CS be guaranteed, SOPs should be drawn up for development and structured documentation (e.g. coding standards).</p>		[2.2] [2.3] [5.2]
<ul style="list-style-type: none"> • Creating user and system manual 		
<p>The <u>user manual</u> should be written such that operation of all functions of the system is clear to users. The user should be able to use the system correctly solely by reading the manual. The manual should be created by IT professionals in co-operation with users.</p>		[2.2] [2.3] [5.2]
<p>The <u>system manual</u> for the system administrators should describe all tasks that are necessary for routine operation of the CS. The tasks described in this manual should normally be carried out by IT professionals.</p>		

<ul style="list-style-type: none"> • Installation and operation 	<p>[2.2] [2.3] [5.2]</p>
<p>The following instructions should be prepared for installation and putting the CS into operation:</p> <ul style="list-style-type: none"> ♦ Installation plan ♦ Training plan (see section 1.3 "Personnel") ♦ Plan for putting the system into operation 	<p>[3.1]</p>
<p>After installation, checks should be carried out to ensure that the installation has been carried out according to the installation plan (IQ, Installation Qualification). The environment requirements for the CS should be described. Measures to avoid the effects of fire, water, dust and mechanical and magnetic effects should be defined.</p> <p>If viruses are known to exist for the operating systems for the CS in question, data media should be scanned for viruses prior to installation.</p>	<p>[2.2] [2.3] [5.2] [7.1]</p>
<ul style="list-style-type: none"> • Planning and conducting acceptance tests <p>See "Planning and execution of acceptance tests" under section 2.2.</p>	<p>[2.2] [2.3] [5.2] [7.1]</p>
<ul style="list-style-type: none"> • Release <p>A CS is held to be validated when the quality plan has been completely and correctly followed and the desired results have been obtained. Following this, the CS is formally released for operation. The conformity to the quality plan must be checked by a final review.</p> <p>Should the CS not adhere to the specifications in non-critical points (see "Risk analysis"), provisions may be made to still use the system after making due reference to such points and introducing suitable organisational workarounds if necessary.</p> <p>Parallel operation of the CS in conjunction with the previous, manually operated system should be considered if using a new technology continues to present an identifiable risk despite proper development in accordance with the life-cycle model.</p>	<p>[2.2] [2.3] [5.2]</p> <p>[2.1] [7.2]</p>
<ul style="list-style-type: none"> • Operation <li style="padding-left: 20px;">♦ Change control <p>Changes must be approved by the responsible person as detailed in the quality plan.</p> <p>In the event of changes to a CS the life-cycle defined in the validation plan should be followed. The entry phase into the life-cycle and the exit phase from the life-cycle should be defined for each change. The entry and exit phases and all phases between these points should be traversed in the case of a change in accordance with the SOPs defined in the quality plan. This dictates the procedures in the event of a change.</p> <p>The decision to revalidate the entire system following a change should be examined on a case-by-case basis depending on the complexity of the CS and the significance of the change in respect of GMP. The <i>risk analysis</i> should be taken as a basis for this decision.</p>	<p>[11]</p> <p>[2.2] [2.3]</p>

◆ System monitoring and maintenance	
<p>The correct operation of the CS including peripherals should be monitored continuously according to a fixed plan and documented in log books. The log books should be stored as part of the life-cycle documentation.</p> <p>In order to keep the system in operation, preventive maintenance measures should be described which should be designed to cope with the specific causes of possible system failure. See section 6 for measures for the residual risk of system failure.</p>	[16]
◆ Error handling	
<p>See section 6 for error handling If eliminating the error involves changing the CS, the procedure described under "Change control" should be followed.</p>	[15-17] [11]
• Phase out	
<p>The phase out is a formal act of discontinuing a system, marking the end of the life-cycle. The potential impact on existing systems and data should be examined prior to withdrawal.</p> <p>The documentation storage period should be based on the storage period required for the manufacturing documentation for the last batch of finished drugs affected by the system.</p>	[2.2] [2.3]

2.2 **Cross-phase activities**

- Planning and conducting tests

The following tests should be planned and executed:

In the module test, system components are examined for operability on the basis of the system design specifications.

In the integration test, the interfaces between the system components are tested on the basis of the system design specifications.

In the system test in the development environment, the interaction of all system components is tested on the basis of the system design specifications and, if necessary, the user requirements specifications.

In the system test in the application environment (acceptance test), the operational CS is tested on the basis of the user requirements specifications and, if necessary, the system design specifications.

Test methods that can be considered include the *Black-Box test*, the *White-Box test* or a combination of these two methods. A test plan including the following points should be prepared to this end:

- ♦ description of test environment indicating the type and version of hardware and software
- ♦ identification of a test team
- ♦ description of all the proposed tests according to the following scheme:

```
Test objective 1
  Test case 1
    Test specification 1
      Test conditions 1
      Test data 1
      Expected result / acceptance criteria 1
      Description of the test execution 1
      Type of record maintained 1
    ...
    Test specification n
  ....
  Test case m
...
Test objective j
```

The test objectives describe verbally what must be examined and should be derived from the appropriate CS specifications. The extent of examination should be based on the risk analysis (see section 2.1 "Risk analysis").

The relevant test cases are detailed verbal descriptions of the test objective; they should be described such that test specifications can be derived directly from these.

[2.3]

[5.2]

[7.1]

Test specification

The test conditions necessary for the test execution should be determined and the test data with which the test object is exposed.

The expected result or acceptance criteria represent the data or conditions which must be achieved with the test data in accordance with the chosen specifications.

The description of the test execution clearly describes the actions which lead to the test results.

The type of record maintained indicates how the test execution and the test results are documented. Documentation should be such that the entire test procedure can be reproduced by a third party with the requisite know-how.

For the purposes of test evaluation the documented test results are compared with the expected results or acceptance criteria. The tests have been completed once it has been confirmed that the acceptance criteria have been sufficiently met.

"Test" and "testing" are used in this document as a standard term to include OQ (Operational Qualification) and PQ (Performance Qualification).

- Configuration control

A configuration plan describing the following items should be created:

- ◆ nomenclature for the version numbering of the system components and documentation
- ◆ all system components and documents with the respective version numbers and periods of use
- ◆ the tools and procedures to be used to integrate these system components in the desired versions for an operational CS

[4.1]
[5.2]

- Planning and conducting audits

Audits should be conducted periodically to check development and operation of the CS. The activities defined in the quality plan and the outcoming documents should be examined at random on the basis of the relevant SOPs. It should be monitored to ensure that any defects detected are eliminated.

[5.2]

- Planning and conducting reviews

All system components and documents of the life-cycle should be subjected to a review in which their form and content should be verified by a competent person. The verification criteria should be laid down in writing.

[5.2]
[7.1]

A review of the software (source code *review*) should be performed for the functions defined as relevant to GMP following *risk analysis*.

2.3 **Prospective and retrospective validation**

- Prospective *validation*

A CS is held to have been validated prospectively if it has been developed and is operated formally and by content according to the principles of the life-cycle model (see sections 2.1 and 2.2).

[2.1]
[2.2]
[2.3]

- Retrospective *validation*

For existing systems which were not or only partly created in accordance with the principles of the life-cycle model, the following retrospective *validation* procedure should be adopted

[2.1]
[2.2]
[2.3]

- ◆ Prepare an experience report on the past operation of the CS
- ◆ Assess the completeness of the documentation against the life-cycle and evaluate the quality of the documentation (a manufacturer's audit may be required for this purpose)
- ◆ Conduct a *risk analysis* to determine the GMP-relevant components and functions
- ◆ Create a quality plan defining activities and responsibilities
- ◆ Create/revise the documentation necessary for testing the CS
- ◆ Test the GMP-relevant component of the CS in the *risk analysis* using this documentation
- ◆ Release the CS, if necessary implementing additional organizational QA measures
- ◆ Introduce all cross-phase activities/evaluations applicable to the existing system, as in the life-cycle model (see section 2.2)
- ◆ Freeze system status or develop it further according to the life-cycle

[7.1]

3 Access authorization

Each user should only be granted rights to enter, delete or modify data in accordance with his field of work. Procedures for granting these rights should be defined.

[8.1]
[8.3]
[10.2]

Appropriate measures to protect against unauthorized input, deletion or modification of data include user identification in conjunction with authentication. This can be done by physical methods such as granting keys and identity cards or by using personal codes or additionally by restricting access to computer terminals.

[8.2]

The following should be defined for all methods:

- catchment procedure when staff leave or change departments
- substitution in the event of damage or loss
- the correct procedure when personal codes are not available
- maintaining a distribution list

[8.3]

The rules governing generation of a personal code should include details of

- length
- use of special characters and character combinations
- term of validity
- history
- prohibition list

[8.3]

It should be reliably guaranteed that unauthorized third parties cannot access company computerized systems via data transmission lines and networks.

Attempts by unauthorized persons to access company systems should be recorded. The time and the system which an unauthorized person attempted to access but failed should be recorded. These data should be checked regularly.

[8.4]

4 Data input

- Plausibility controls

If technically feasible, the system should perform plausibility controls when data are entered or processed. As the system automatically compares data on input with predefined limits the user should be warned of potential errors when entering the data. There should be no difference between manual input by the user and take-over of data from another system. In the same way, processing operations performed by the system should be checked by the system itself.

[6.1]
[9.2]

- Critical data

Critical data should be defined in the course of risk analysis (see section 2.1 "Risk analysis"). Critical data include all data relevant to product quality.

[9.1]

Input of critical data and their verification should be documented with details of

- ♦ date
- ♦ time
- ♦ user identification
- ♦ action involved

If these data need to be changed, a second person should approve these changes along with the reasons, with the above details, in the *CS* (audit trail). These records should be reviewed regularly.

[10]

Manual input of critical data should be kept to a minimum by using other systems (e.g. input of a batch number via bar code, input of a substance weight by automatic recording of the balance signal). Critical data should be monitored by the system or a suitable system environment.

[9.2]

- Batch release

Where approval of batches for distribution is to be computerized, the system should be able to recognize that only specified persons are authorized to release batches. The required authorization for batch release should be granted with one of the following procedures:

[19]

- ♦ a combination of a physical key (e.g. chipcard, "real" key) and a software key (personal code or another method to guarantee unique identification)
- ♦ an identification step using a software key which must be entered every time a batch is released, in addition to the standard access restrictions (see section 3)

All methods used for identification purposes must be defined, especially regulations for stand-ins.

Following batch release, only the persons granting release and a second named person should be able to make changes to the stored data. The original data must be archived in the system such that it can be reconstructed at any time.

5 Data storage and backup

- Data storage

In the case of electronic filing, details of the format in which the data were stored should also be filed along with the data themselves. In order to generate reliable printouts, an operational print program should be available for every format in the electronic filing system. [12.1]

Before hardware and/or software is exchanged, a change control mechanism should be used to check that the data concerned can also be printed in the new configuration. [13.3]

Should an inevitable change in the hardware and/or software mean that the stored data cannot be printed in the new configuration, then one of the following procedures should be applied:

- ♦ the data in the format concerned should be converted into a format that can be printed in the new configuration
- ♦ the components of the old hardware and/or software configuration required for printing should be retained. In this case it should be guaranteed that a suitable alternative system is available in case the retained system fails.
- ♦ the data is transferred to another medium

The electronically stored data should be checked regularly for availability and integrity. [13.2]

- Data backup

In order to guarantee the availability of the stored data, backup copies should be made of such data that are required to reconstruct all GMP-relevant documentation. This also applies to the system programs required to save and restore the data. [14.1]

The backup procedure must guarantee data integrity. Each backup set should be checked to ensure that it is error-free.

At least two generations of backup copies should be kept. The backup copies should be managed by a suitable system in order to guarantee the availability of the data within an appropriate period. The frequency and extent of backup should be based on the effort involved to recreate the data. This should be defined in the CS specification. [14.1]

Data that cannot be recreated or obtained from other sources should be maintained simultaneously in two storage media during the operation of the CS.

Backup copies should be kept separate from the CS in a different fire protection area. This place should meet the safety requirements, especially in respect of access and environment as defined for the CS. The environment requirements specific to the storage medium should be taken into consideration. Copies of these copies should be made before the expected life of the medium has expired. [13.1]
[14.2]

Backups must be retained for the same period as the original data.

Following changes to the system, change control should ensure the *availability* and *integrity* of the data on the backup copies by restoring the data on a trial basis.

6 Error handling and system failure

Failure of the *CS* is characterized by malfunction or failure of the system components which make proper use of the system impossible in the long term or for an undetermined period. In order to be able to access important data during such periods, substitute systems or alternative ways of presenting the data should be available.

[15-17]

Such systems or procedures should meet the following requirements:

- availability
- practicability
- appropriateness
- efficiency
- reliability
- completeness

These requirements should be defined in advance for every database according to its importance and use and substitute systems should be developed. The permissible time required to start up the emergency system should be derived from the requirements and experience in day-to-day practice, then laid down and, if necessary, contractually agreed.

In the event of a system failure there should be a general procedure to restore the hardware or software from any situation to a correctly functioning and basic condition and to reconstruct the relevant data reliably.

With growing operational experience with a *CS*, thought should be given to the possibility of establishing detailed solutions for known, well defined system failures.

In order to remedy quickly or avoid system errors, appropriate control measures should be applied to allow early identification of an imminent breakdown and initiation of a remedy.

A procedure to remedy system errors should consider the following:

- conduct error analysis
- commission and carry out repairs
- implement additional organizational measures (work around)
- test software components
- check stored data
- reconstruct data
- system release for re-use
- documentation instructions

It should be confirmed that the tests and review procedures to be used are reliable.

7 Annex

7.1 *Supplementary guideline for computerized systems: Annex 11¹*

Definitions

Computerized system:

[0.1] A system including the input of data, electronic processing and the output of information to be used either for reporting or automatic control.

System:

[0.2] Is used in the sense of a regulated pattern of interacting activities and techniques which are united to form an organized whole.

Principle

[0.3] The Introduction of computerized 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. [0.4] Where a Computerized system replaces a manual operation, there should be no resultant decrease in product Quality or quality assurance. [0.5] Consideration should be given to the risk of losing aspects of the previous system by reducing the involvement of operators.

Personnel

1. [1.1] It is essential that there is the closest cooperation between key personnel and those involved with Computer Systems. [1.2] Persons in responsible positions should have the appropriate training for the management and use of systems within their field of responsibility which utilizes Computers. [1.3] This should include ensuring that appropriate expertise is available and used to provide advice on aspects of design, validation, installation and operation of computerized system.

Validation

2. [2.1] The extent of validation necessary will depend on a number of factors including the use to which the system is to be put, whether it is prospective or retrospective and whether or not novel elements are incorporated. [2.2] Validation should be considered as part of the complete life cycle of a computer system. [2.3] This cycle includes the stages of planning, specification, programming, testing, commissioning, documentation, operation, monitoring and changing.

System

3. [3.1] Attention should be paid to the siting of equipment in suitable conditions where extraneous factors cannot interfere with the system.
4. [4.1] A written detailed description of the system should be produced (including diagrams as appropriate) and kept up to date. [4.2] 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.
5. [5.1] The software is a critical component of a computerized system. [5.2] 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.
6. [6.1] The system should include, where appropriate, built-in checks of the correct entry and processing of data.

¹ The authors have numbered the sentences in square brackets to allow more precise referencing.

7. [7.1] 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. [7.2] If a manual system is being replaced, the two should be run in parallel for a time, as part of this testing and validation.
8. [8.1] Data should only be entered or amended by persons authorized to do so. [8.2] Suitable methods of deterring unauthorized entry of data include the use of keys, pass cards, personal codes and restricted access to computer terminals. [8.3] There should be a defined procedure for the issue, cancellation, and alteration of authorization to enter and amend data, including the changing of personal passwords. [8.4] Consideration should be given to systems allowing for recording of attempts to access by unauthorized persons.
9. [9.1] 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. [9.2] This check may be done by a second operator or by validated electronic means.
10. [10.1] The system should record the identity of operators entering or confirming critical data. [10.2] Authority to amend entered data should be restricted to nominated persons. [10.3] Any alteration to an entry of critical data should be authorized and recorded with the reason for the change. [10.4] Consideration should be given to the System creating a complete record of all entries and amendments (an "audit trail").

11. [11.1] 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. [11.2] 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. [11.3] Every significant modification should be validated.
12. [12.1] For quality auditing purposes, it shall be possible to obtain meaningful printed copies of electronically stored data.
13. [13.1] Data should be secured by physical or electronic means against wilful or accidental damage, and this in accordance with item 4.9. of the Guide. [13.2] Stored data should be checked for accessibility, durability and accuracy. [13.3] 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. [14.1] Data should be protected by backing-up at regular intervals. [14.2] Back-up data should be stored as long as necessary at a separate and secure location.
15. [15.1] There should be available adequate alternative arrangements for systems which need to be operated in the event of a breakdown. [15.2] The time required to bring the alternative arrangements into use should be related to the possible urgency of the need to use them. [15.3] For example, information required to effect a recall must be available at short notice.
16. [16.1] The procedures to be followed if the System falls or breaks down should be defined and validated. [16.2] Any failures and remedial action taken should be recorded.
17. [17.1] A procedure should be established to record and analyze errors and to enable corrective action to be taken.
18. [18.1] 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).
19. [19.1] When the release of batches for sale or supply is carried out using a computerized system, the system should recognize that only a Qualified Person can release the batches and it should clearly identify, and record the person releasing the batches.

7.2 Glossary

Audit Trail

Control mechanism of the system that allows all data entered and further processed by the system to be traced back to the original data.

CS

Computerized system in accordance with the "definitions" in Annex 11.

Review

Complete review of a system component or document for form and content by another competent person.

Risk analysis

Methodical procedure to analyse processes, systems or programs in sufficient detail and to examine the resulting sub-units in respect of the results and effects on a (pharmaceutical) product.

Validation

Documented records, in compliance with the principles of GMP, that procedures, processes, equipment, materials, operations or systems actually produce the desired results.

Test methods

With the Black-Box Test, the test cases are derived solely from the description of the test object, the inner structure of the object is thus not considered when creating the test plan.

With the White-Box Test the test cases are derived solely from the structure of the test object.

With the Source-Code Review the source code is checked against the documentation describing the system by one or several professionals.

Safety

The *safety* of a CS is reflected by the confidentiality, integrity and availability of the system.

Integrity

Protection against unauthorized changes to information.

Availability

Protection against unauthorized retention of information.

7.3 **References**

This guideline is based on the experience of the members of the APV Specialist Section and the following sources:

[Note that some of these references duplicate entries in Appendix T. They are included here for completeness.]

1. Feiden K. (Hrsg)
Betriebsverordnung für Pharmazeutische Unternehmer
Deutscher Apotheker Verlag, Stuttgart 4.Aufl. 1995
2. Die Regelung der Arzneimittel in der Europäischen Gemeinschaft; Band IV; Leitfaden einer Guten Herstellungspraxis für Arzneimittel; Kommission der Europäischen Gemeinschaften; 1992
and
EU Leitfaden einer Guten Herstellungspraxis für Arzneimittel (III/2244/87 Rev 3, Jan 1989)
in: Auterhoff G. (Hrsg)
EG-Leitfaden einer Guten Herstellungspraxis für Arzneimittel
2. Aufl. , Editio Cantor Aulendorf 1993
3. EC-Commission
Working Party on "Control of Medicines and Inspections"
Supplementary guidelines for computerized systems
(III/8263/89-EN) Final Draft 1991 (Part of Guide to GMP)
4. Leitfaden einer Guten Herstellungspraxis der PIC
Bekanntmachung von ergänzenden Leitlinien zum Leitfaden der Guten Herstellpraxis der Pharmazeutischen Inspektions Convention:
Ergänzende Leitlinien für computergestützte Systeme
BAnz Nr 18, S 466 v. 28.1.92
5. ISO 9000 Teil 3
Leitfaden für die Anwendung von ISO 9001 auf die Entwicklung, Lieferung und Wartung von Software, Beuth Verlag, Berlin 1992
6. DGQ-NTG Schrift Nr. 12-51
Software-Qualitätssicherung
Beuth Verlag, Berlin, Köln 1986
7. DGQ-ITG Schrift Nr. 12-52
Methoden und Verfahren der Software-Qualitätssicherung
Beuth Verlag, Berlin 1992
8. Kriterien für die Bewertung der Sicherheit von Systemen der Informations-technik (ITSEC); Vorläufige Form der harmonisierten Kriterien; Amt für amtliche Veröffentlichungen der Europäischen Gemeinschaften; 1991

9. UK Pharmaceutical Industry Computer Systems Validation Forum
Good Automated Manufacturing Practices
Supplier Guide for Validation of Automated Systems in Pharmaceutical Manufacture, 2nd Draft January 1995
10. Therapeutic Goods Administration
Use of Computers
Australian Code of GMP for Therapeutic Goods - Medicinal Products -
Part 1, Section 9, January 1993
11. Matsuda T.
Guideline on Control of Computerized Systems in Drug Manufacturing
J Pharm Sci & Technol 48, 11 (1994)
12. FDA
Code of Federal Regulations CFR21
April 1988
13. FDA
Guide to Inspection of computerized systems in drug processing ("blue book")
Reference Materials and Training Aids for Investigators
US Dept. of Health and Human Services, FDA, Feb. 1983
14. FDA
Draft Guide to the Inspection of Software Development Activities
Reference Materials and Training Aids for Investigators
US Dept. of Health and Human Services, FDA, 1987
15. FDA: COMPLIANCE POLICY GUIDE 7132a07
Computerized drug processing -- input/output checking
National Technical Information Service, Springfield, 1988
16. FDA: COMPLIANCE POLICY GUIDE 7132a08
Computerized drug processing -- i.d. of "persons"
National Technical Information Service, Springfield, 1988
17. FDA: COMPLIANCE POLICY GUIDE 7132a11
GMP applicability to hardware and software
National Technical Information Service, Springfield, 1988
18. FDA: COMPLIANCE POLICY GUIDE 7132a12
Computerized Drug Processing; Vendor Responsibility
National Technical Information Service, Springfield, 1988

19. FDA: COMPLIANCE POLICY GUIDE 7132a15
Source code for process control application programs
National Technical Information Service, Springfield, 1988