

Foreword:

This document is a nonbinding and nonofficial translation of the so called Aide Memoire (Ref. #: 07121202) of the German ZLG (Central Authority of the Laender for Health Protection). The ZLG is the central coordination unit of the German Laender (federal states) regarding medicinal products for human and animal use. For the control of medicinal products in Germany the ZLG is also hosting so called Subject Experts Groups, which are manned by German GMP/GDP inspectors dedicated to special topics. The group number 11 (EFG11) was established to address the European requirements based on the GMP Guidelines - Annex 11 - for computerized systems. The members of the Subject Expert Group # 11 are top-notch specialists and experienced GMP/GDP field inspectors.

Documents by the ZLG, titled as "Aide Memoire", can be interpreted as (non-binding) "inspection guidance documents" written by a ZLG Subject Expert Group for other GMP/GDP inspectors, which are not highly specialized in such special topics, but who should include these into a GMP/GDP inspection. In other words, Aide Memoires are written by inspectors for inspectors. Also each Subject Expert Group can decide to make any Aide Memoire available for the public or only for internal use within the German inspectorates.

With the revisions 2011 of GMP Chapter 4 and Annex 11, based on the rationale "in the light of the increasing use of electronic documents within the GMP environment" it was decided that the Aide Memoire for inspections of computerized systems will be made available for the public in 2013. The officialese of the ZLG and inspectorates is the German language, so the Aide Memoire was written and published in German language only.

It is assumed that irrespectively to which agency an inspector belongs to, e.g. Germany, any other Member State of the European Union, PIC/S member state, ICH members, MRA state, etc.; they will do inspections in an similar or almost identical way. And it might be oriented on this Aide Memoire – or not. It can mainly be used to understand the current thinking, expectations, or interpretation of Annex 11 of inspectors, which is just a juristically law text / rule, with statements for example "IT infrastructure should be qualified" or "Regular back-ups of all relevant data should be done". A law or rule is not defining the "how-to" as detailed instructions, and an inspector will not ask "have you implemented ITIL?" or "Are you making incremental backups daily?".

Inspectors do know such guidance documents like the ISPE GAMP 5 standard, but the baseline for inspections are always the predicate rules. Within a communication between industry and inspector it is always beneficial to have a clear understanding of the expectations, roles, and mind-sets of each party. An inspection itself is a special communication type including understanding and realizing cognitive expectations of expectations of each party. The complex circumstance where Good Manufacturing Practice meets the diverse fields of IT and Software require a bilateral communication and grasp model. On the other hand it is not the duty of an inspector to tell the industry how to do things in detail, to act like a consultant, or making public advises or statements. The focus of an inspection is to measure and rate the level of compliance.

In this context the current Aide Memoire is even more important and should be read in such a way, that it gives an insight into the inspectors' thinking, which should be understood just as one possible way of interpretation and does also not guarantee a successful inspection. In general inspections have a wider range of compliance verifications and contents, e.g. process validation, quality risk management, recalls, etc. . Therefore the Aide Memoire can also not be used as a simple tick-box checklist for implementation by the industry, but should be used to prepare inspections in order to understand such expectations of expectations properly.

We think that the intention of the inspectors for providing the Aide Memoire to the public was based on such an exchange of information and to cultivate ways of understanding. The purpose section of the Aide Memoire states also that it can not represent an up-to-date and consistent statement and it is recommended to involve members of the Subject Matter Group in the case of any discussion needs.

We also think that just by occupying oneself with such expectation statements do improve the communication platform during inspections, avoiding misunderstandings or misinterpretations, which are both leading to extra efforts and to a lower outcome of inspections. If possible expectations are mapped in the forefront of inspections the efficiency and added value of inspections can be increased; at the end of the day the objective is to take seriously care of patient safety and product quality. Instead of wasting time for finding the right meaning or intentions of questions, it should be the objective to setup a proper communication and information exchange platform.

The current Aide Memoire does contain example questions, which may be asked during an inspection, for example "Which qualification does IT personnel have?". Most of the questions are defined as open (or even vague) questions - not as simple closed questions - , so the answers to be given should be accordingly detailed, understandable, based on a defined rational, and transparent.

During the translation we found sometimes different possible meanings or interpretations of the questions – or some technical descriptions are very frugal or simplified. If two different or even opposite disciplines are meeting in an inspection, it is very important to define the way of presenting regulatory requirements and technical details & implementation. If for example controls of the entire IT network would be examined, then it might confuse more if a huge, multi-page network layout is presented.

The aim of this document is to provide an accurate translation of the Aide Memoire from German into English language to a wider audience. Except of the PIC/S PI-011 (chapter 24) from 2007 or some Questions and Answer or FAQs web blogs published by some agencies we do not notice any similar documents presented to the public. Hence this Aide Memoire translated into English language can be seen as a beneficial source or impulse for any expert in our industry.

We decided to make a specialist but free translation, instead of a word-by-word translation, in order to reflect the correct meaning and spirit. Text in **blue color** is indicating additions by us, in order to improve the tangibility or the exactness of statements, or in special cases adding notes or remarks by us. None of them can cover all cases and variants and constitute an ultimatum for all times. And here we are again: A rule requires an interpretation, which defines goals or expectations, resulting into a concept or approach and finally in integration. Maybe this is also a part of knowledge management and an exchange of experience and expertise. If you are an expert, freshman, or an inspector please feel free to contact us for any comment or remark to our translation at talk@comes-services.com. We appreciate any feedback and like to update this document.

Related to the IT topics and its continuously and faster improvements of technology and evolving best practice standards we might have concerns that this special topic might only be understandable and assessable by some subject matter experts for the future. It might be an ambitious goal to simplify the requirements and improve information exchange. It seems to be nearly impossible to find one single expert for all related fields, e.g. having all standards in mind like ITIL (ISO20.000), PMBOK, SCRUM, CMMI, ISO standards and all typical GMP requirements (PQS, ICH, QRM, etc.).

At the end we decided to publish this translation and we welcome any feedback to it.

Thank you for reading, commenting and thinking about it.

Disclaimer:

This translation of the Aide Memoire of the ZLG is meant to assist pharmaceutical manufacturing companies in managing GMP regulated systems. CCS cannot ensure and does not warrant that a system managed in accordance with this translation will be acceptable to any regulatory authorities. Further, this Aide Memoire does not replace the need for hiring professional personnel, training, and/or consultancy.

[Begin of Translation on next page](#)

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 2 of original |
| Nonbinding translation by CCS | | ZLG |

Table of contents:

1 Purpose 4

2 Inspections of computerized systems 5

 2.1 Principles 5

 2.2 General 6

 2.2.1 Risk Management 6

 2.2.2 Personnel 9

 2.2.3 Suppliers and Service Providers 11

 2.3 Project Phase 13

 2.3.1 Validation 13

 2.4 Operational Phase 20

 2.4.1 Data 20

 2.4.2 Accuracy Checks 21

 2.4.3 Data Storage 24

 2.4.4 Printouts 26

 2.4.5 Audit Trails 27

 2.4.6 Change and Configuration Management 30

 2.4.7 Periodic evaluation 31

 2.4.8 Security 33

 2.4.9 Incident Management 37

 2.4.10 Electronic Signature 38

 2.4.11 Batch release 40

 2.4.12 Business Continuity 42

 2.4.13 Archiving 44

3 Definitions and abbreviations 45

4 Attachments and Forms 45

| | | |
|----------------------------------|--|---------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 3 |
| Nonbinding translation by CCS | | ZLG |

1 Purpose

In the first part this Aide-Mémoire (short: AiM) contains a short introduction for the inspection of computerized systems. The second part contains explanations of the EU GMP Annex 11 requirements and commented questions which can be asked during an inspection. These given comments should be the basis for the rating of receiving answers. This structure / approach should simplify the inspection of computerized systems (short: CS).

The structure of both parts of the questionnaire and related comments is oriented on the EU GMP Annex 11 „computerized systems“. Each section contains the original text of Annex 11 (here in English language) in *italic text*. As far as required references to the related EU GMP Chapter 4 – Documentation – are included.

NOTE:

- “EU GMP” full reference: EudraLex - Volume 4 Good manufacturing practice (GMP) Guidelines – Annex 11 and Chapter 4 in revision 1 (from 2011) by the European Medicines Agency (short: EMA).
- The German Version of Annex 11 contains the translation of Annex 11 by the ZLG (not by the German BMG)

In addition the AiM contains sections of the definitions and abbreviations of the related Annex 11 Glossary. In some companies such terminology can differ from these. For example, Annex 11 is using the terms of „Validation“ and „Qualification“, but not the term of “Verification”.

Because of the continuous developments of regulations for the area of computerized systems this AiM can not represent an up-to-date and consistent statement. Therefore in any case of doubt it is recommended to involve members of the ZLG Subject Expert Group (German: Expertenfachgruppe 11 „Computergestützte Systeme“ – short: EFG 11).

Further information can be found on the EMA website - section „Regulatory / Human medicines / Inspections / GMP/GDP compliance / Q&A“ and in the so called “votes” of the EFG 11.

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 4 of original |
| Nonbinding translation by CCS | | ZLG |

2 Inspections of computerized systems

2.1 Principles

Principle (Annex 11)

This annex applies to all forms of computerised systems used as part of a GMP regulated activities. A computerised system is a set of software and hardware components which together fulfill certain functionalities.

The application should be validated; IT infrastructure should be qualified.

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 the process.

2.1 Principles

| No. | Related Questions | Comments |
|------------|--|-----------------|
| | In revision 1 of Annex 11 the term of a computerized system was redefined compared to the previous (initial) version. It should be noted in this instance, that the subject is not only limited to the software and hardware parts, but rather related to the functionality – in the meaning of the (GMP) processes ¹ . Such processes may include process control, data processing or documentation (recording). | |
| | Annex 11 is covering all sorts of computerized systems and at a minimum during an initial (first) inspection a first impression of the systems landscape ² can be derived from an inventory list, and how GMP- criticality is assessed (ref. No. 4.3 Annex 11). | |
| | The terminology of validated applications and qualified IT infrastructure is consistent with the terms used for process validation and equipment / device qualification (reference to the German AMWHV given). | |
| | The benchmark of Annex 11, revision 1 between expected safety (risks) of manual processes compared to automated processes stays unchanged. | |

¹ Defined by the word “applications“ should be validated.

² System landscape contains a layer model of the IT Infrastructure and Applications. It is interesting that standards like ITIL, CMMI or ISO 20.000/27.000 are not mentioned. In the entire Aide Memoire the term “system” is very often used, also it should be understood as “application”.

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 5 of original |
| Nonbinding translation by CCS | | ZLG |

2.2 General

2.2.1 Risk Management

1. Risk Management - Annex 11

Risk management should be applied throughout the lifecycle of the computerised system taking into account patient safety, data integrity and product quality. As part of a risk management system, decisions on the extent of validation and data integrity controls should be based on a justified and documented risk assessment of the computerised system.

2.2.1 Risk Management

| No. | Related Questions | Comments |
|----------------|---|-----------------|
| 2.2.1.1 | A risk management system covering computerized systems should be established and should be integrated into the Pharmaceutical Quality System (PQS) in order to assure GMP-compliance. This risk management system should cover all GMP-related aspects, such as patient safety, data integrity and product quality. Risk management should be applied throughout the full lifecycle of the computerised system. | |
| 2.2.1.2 | The basis for the operation of a computerized system in any GMP area should be a profound and documented risk assessment based on pre-defined, justified and traceable criteria; by means of methods and approaches which analyze computerized systems to a sufficient level of detail regarding outcomes and impacts to the (pharmaceutical) product, patient safety, quality of data sets and data integrity. | |
| 2.2.1.3 | The results (outcomes) of a risk assessment are the basis for the decisions about the scope of validation and to safeguard data integrity and data quality. | |
| 2.2.1.4 | Particularly with regard to changes of the computerized system during the project phase a re-assessed appraisalment should be executed. However risk assessments should be periodically (re-)executed. The extent of risk assessments should depend on the change type and the criticality of the computerized system. | |

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 6 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.2.1 Risk Management | | |
|------------------------------|--|--|
| No. | Related Questions | Comments |
| 2.2.1.5 | What is the relationship (or impact) between computerized systems or processes to patient and product safety, or electronic data quality or integrity? | On the basis of this question critical systems can be identified. These are in scope of the major objective of the inspection. For example, such systems are controlling production process systems (e.g. reactor supervision, filling lines, blender) or systems used in the nearer production areas (e.g. Air Handling Units / HVAC, CIP-/SIP- processes, WFI or Aqua Purificata production) or in the area of quality control (HPLC, analytical instruments for IPC, data for batch releases). |
| 2.2.1.6 | Which actions have been addressed for risk mitigation / reduction during the risk assessment(s)? | In some cases all relevant GMP requirements can not be fulfilled by an existing system for technical reasons (restrictions). Within the scope of a risk control process there might exist additionally defined actions or the operational range was limited. A replacement of such systems should be initiated (refer to section <u>validation</u>) |
| 2.2.1.7 | Which statements (declarations) are defined in higher-level QA-documents regarding the identification and evaluation of risks? | The management (handling) of computerized systems must be included in the related Quality System. |
| 2.2.1.8 | Which exigent and prospective risk reduction actions can be derived out of these? | The fundamental management of risk reduction and avoidance should be defined in the QA system. |
| 2.2.1.9 | To what extent have GMP related processes been assessed for the type and range of validation activities by the risk assessment(s)? | During the risk assessment the direct and indirect impact of the computerized system regarding GMP should be analysed. Critical processes and functions, which have been identified, might be subject of a separate / dedicated inspection (part). (refer to section <u>validation</u>) |

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 7 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.2.1 Risk management | | |
|------------------------------|--|---|
| No. | Related Questions | Comments |
| 2.2.1.10 | Was a risk assessment executed in the case of a retrospective validation? | At minimum following actions are expected for a retrospective validation approach: <ul style="list-style-type: none"> - Execution of a risk analysis in order to evaluate GMP relevant parts of the system and to define additional actions, - Analysis and evaluation of historic data - Test execution of the as critical ranked GMP relevant parts. (refer to section <u>validation</u>) |
| 2.2.1.11 | In which way are risk assessments for computerized systems implemented to the change control system? | Changes should be investigated towards the (potential) risks (by/for the computerized systems). |
| 2.2.1.12 | To what extent is risk management implemented in the respective phases of the system life cycle? | Risk management should be applied throughout the entire system lifecycle. By the initial assessment the GMP criticality should be analysed. Especially the impact on patient safety, data integrity and product quality should be evaluated. The User Requirement Specification(s) should be developed on the basis of potential risks. These form the basis of the first initial risk ranking. Complex systems should be based on a detailed risk assessment, resulting in the identification of critical functions. This should assist to address all critical functions during validation. Risk management includes the implementation of control strategies and its verification. ³ |
| 2.2.1.13 | Does the recognizability of risks have any impact on the overall risk? | Only risks, which have been detected, can result in the reduction of the overall risk. |

³ This implies that several risk areas should be addressed – GMP risk, functional / technical implementation risks, and for example system development risks.

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 8 of original |
| Nonbinding translation by CCS | | ZLG |

2.2.2 Personnel

2. Personnel - Annex 11

There should be close cooperation between all relevant personnel such as Process Owner, System Owner, Qualified Persons and IT. All personnel should have appropriate qualifications, level of access and defined responsibilities to carry out their assigned duties.

2.2.2 Personnel

| No. | Related Questions | Comments |
|----------------|--|---|
| 2.2.2.1 | All relevant personnel should be sufficiently trained in the operations and management of computerized systems within the defined area of responsibilities. In particular personnel (e.g. IT employees respectively system administrators), which are responsible for planning, development, programming, validation, installation, operation, maintenance or decommissioning of computerized systems, should have sufficient expertise. Such expertise should be regularly improved by skill enhancement and further trainings. There should be close cooperation between all relevant personnel. | |
| 2.2.2.2 | In order to execute the related duties by employees there should be defined responsibilities and sufficient access rights. | |
| 2.2.2.3 | Access rights should only be assigned to employees, which are adequately trained. | |
| 2.2.2.4 | Data input or changes should only be executed by personnel, which are adequately trained referring to such actions. | |
| 2.2.2.5 | Which qualification does IT personnel have? | The basis GMP principle, that personnel should only be employed based on their knowledge and expertise/capabilities, does also apply to IT- personnel. |
| 2.2.2.6 | How is the personnel trained? In which way do training plans contain requirements for the usage of computerized systems? | The responsible personnel needs to assure, that the handling (operation) of the computerized system by the assigned users is based on GMP rules and the (firm's) internal work instructions. Personnel, which is appointed to a computerized system (work station), must be familiar with the work processes itself and the rational decision-making process in case of an error situation to identify and decide between self-help or the need of involvements of internal or external support. On the basis of the training plan it should be detectable, that IT-specific topics are also covered. |
| 2.2.2.7 | To what extent are GMP topics covered in trainings for IT personnel? | In particular IT personnel should be trained in the topics of documentation (practices) and change control processes. |

| | | |
|----------------------------------|--|-------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 9 of original |
| Nonbinding translation by CCS | | ZLG |

2.2.2 Personnel

| No. | Related Questions | Comments |
|-----------------|---|---|
| 2.2.2.8 | Which persons / roles are involved in the development, planning and implementation of computerized systems? | The assignment of system- and process owners (persons in charge) is the current / recommended practice. |
| 2.2.2.9 | How are such responsibilities defined for the involved persons (parties)? | A critical question can be asked, if these defined responsibilities are mapped by the appropriate competence levels/capabilities. |
| 2.2.2.10 | Which persons are permitted to enter or change data? | The input or modification of data should only be possible for users which have the corresponding permissions and training. Permissions should only be granted to persons, which are assigned to an individual system according their job / place of work description. A critical question can be asked, which persons are allowed to change / modify data and how the change process is designed. |
| 2.2.2.11 | How far are Qualified Persons (QPs) involved / engaged? ⁴ | The QP should be involved at least for the release (go-live decision, e.g. validation report) of a system, if it creates or processes batch release relevant data (refer EU GMP Annex 16). |

⁴ Maybe one of the most important questions. Refer also to revised Chapter 2 Personnel (Deadline for coming into operation: 16 February 2014).

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 10 of original |
| Nonbinding translation by CCS | | ZLG |

2.2.3 Suppliers and Service Providers

3. Suppliers and Service Providers -Annex 11

3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogous.

3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment.

3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.

3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.

2.2.3 Suppliers and Service Providers

| No. | Related Questions | Comments |
|---------|--|---|
| | | 3.1 When third parties (e.g. suppliers, service providers) are used e.g. to provide, install, configure, integrate, validate, maintain (e.g. via remote access), modify or retain a computerised system or related service or for data processing, formal agreements must exist between the manufacturer and any third parties, and these agreements should include clear statements of the responsibilities of the third party. IT-departments should be considered analogously. |
| 2.2.3.1 | Which duties are defined on a contractual basis? | Contracts should unambiguously and clearly indicate the roles and responsibilities. Response times should be predefined. |
| 2.2.3.2 | Which persons are involved? | At least the process owner and the system owner should be involved during the phase of the contract design. |
| 2.2.3.3 | What is the firm's definition of a Service Provider? | As Service Providers are all parties understood, who provide any services irrespective if they belong to an independent (external) enterprise, to the same company group/structure or an internal service unit. |
| | | 3.2 The competence and reliability of a supplier are key factors when selecting a product or service provider. The need for an audit should be based on a risk assessment / ranking. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 11 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.2.3 Suppliers and Service Providers | | |
|--|--|---|
| No. | Related Questions | Comments |
| 2.2.3.4 | How was the qualification / assessment of a supplier respectively service provider conducted? | References (testimonials) or certifications can be applied. Any certification (in the meaning of third party certifications) can not replace/supersede a supplier qualification. ⁵ Methods of supplier qualifications can be for example a history report of previous deliveries or service provisions, transfer and assessment of questionnaires (postal audits) or supplier/vendor audits. |
| 2.2.3.5 | Was a supplier audit executed? | It should be defined internally under which conditions a supplier audit needs to be executed. In general supplier audits should be executed for software, which belongs to category 5 (refer to ISPE GAMP 5 – Bespoke / Custom Software). |
| <i>3.3 Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to check that user requirements are fulfilled.</i> | | |
| 2.2.3.6 | How was the verification executed to check whether the standard (off-the-shelf) product fulfils the user requirements? | There should exist a documented assessment of the user requirements against the system documentation provided by the supplier. Deviations should undergo a risk evaluation. |
| <i>3.4 Quality system and audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.</i> | | |
| 2.2.3.7 | The supplier evaluation, the functional specification and further qualification documents should be in place in a plausible way and chronological order. Audit reports should exist for review (to provide an insight into the audit processes). | |

⁵ Important.

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 12 of original |
| Nonbinding translation by CCS | | ZLG |

2.3 Project Phase

2.3.1 Validation

| |
|---|
| <p>4. Validation - Annex 11</p> <p>4.1 <i>The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.</i></p> |
| <p>4.2 <i>Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.</i></p> |
| <p>4.3 <i>An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.</i></p> |
| <p>4.4 <i>User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.</i></p> |
| <p>4.5 <i>The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.</i></p> |
| <p>4.6 <i>For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.</i></p> |
| <p>4.7 <i>Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.</i></p> |
| <p>4.8 <i>If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.</i></p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 13 of original |
| Nonbinding translation by CCS | | ZLG |

2.3.1 Validation

| No. | Related Questions | Comments |
|--|---|---|
| 2.3.1.1 | „The application should be validated; IT infrastructure should be qualified.“ (Annex 11 – principle) | |
| 2.3.1.2 | The qualification of the IT infrastructure is henceforth a concrete requirement of Annex 11. The perception of this requirement is assigned to the system owner (typically to the IT department). | |
| 2.3.1.3 | Are instructions in place, which define the requirements of the IT Infrastructure qualification? | For example specifications for servers, scanners, switches, printers, and SOPs and Plans / Protocols for the qualification. |
| <i>4.1 The validation documentation and reports should cover the relevant steps of the life cycle. Manufacturers should be able to justify their standards, protocols, acceptance criteria, procedures and records based on their risk assessment.</i> | | |
| 2.3.1.4 | Life cycle phases are Planning, Realisation, Validation, Operation, and Decommissioning of systems. It is expected that the GMP criticality is assessed first on the system level on the basis of a SOP or checklist. There are several methods for software development (e.g. V-model, "rapid prototyping") and depending on these related validation approaches. Applied methods should be represented and justifiable. | |
| 2.3.1.5 | On the question regarding the validation of the application / software the company's answer refers to the acquisition and installation of a validated software solution. How can such a statement replied? | Validation of software is solely possible in the specific application area. Basic functions can be tested and verified by the supplier. For such cases the corresponding documentation should be available and assessed. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 14 of original |
| Nonbinding translation by CCS | | ZLG |

2.3.1 Validation

| No. | Related Questions | Comments |
|--|---|--|
| 2.3.1.6 | <p>What validation methodology was used as a basis?</p> <p>What essential validation phases were applied?</p> <p>Which documents were created in the scope of the validation?</p> | <p>The validation approach according the V-model is commonly used. Following document are expected:</p> <ul style="list-style-type: none"> - Creation of a Validation Plan, - Setting up User Requirements / User Requirement Specification - Selecting a supplier on the basis of the User Requirements, - Creation of a Functional Specification on the basis of the user requirements (generally created by the supplier). - Risk analyses (plural) - Installation, - Installation Qualification (IQ), - Operational Qualification (OQ), - System Test and if applicable assessment of supplier's test documentation, - Performance Qualification (test execution in the operational environment under operational conditions), - Instructions (Specifications) and corresponding Reports of the essential phases (see above). <p>If alternative models were chosen, fit for purpose should be checked .</p> |
| 2.3.1.7 | <p>What is the effect of the risk evaluation on the scope of validation?</p> <p>In which extent was the scope of validation according the results of the risk assessment adjusted?</p> | <p>Compare the scope of validation between a critical and a non-critical process / functions.</p> |
| <p><i>4.2 Validation documentation should include change control records (if applicable) and reports on any deviations observed during the validation process.</i></p> | | |
| 2.3.1.8 | <p>How were changes during the software development and validation phase performed and reproducible documented (documented evidence)?</p> | <p>A less formal change management process is during this phase expected, compared to the operational phase. It is imperative that changes before go-live are traceable.</p> <p>The setup of the approval process might be plainly reduced, compared to the operational phase.</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 15 of original |
| Nonbinding translation by CCS | | ZLG |

2.3.1 Validation

| No. | Related Questions | Comments |
|--|---|--|
| 2.3.1.9 | How are detected deviations managed and documented during the validation (e.g. test results not conform to specifications)? | It is expected, that deviations are documented and assessed by the responsible person (process owner, system owner). GMP critical deviations should be closed before go-live. If deviations are not closed, these should be evaluated and the reason / rational should be documented. |
| <i>4.3 An up to date listing of all relevant systems and their GMP functionality (inventory) should be available. For critical systems an up to date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software pre-requisites, and security measures should be available.</i> | | |
| 2.3.1.10 | What computerized systems are in operations? What purpose / functionality are covered by these systems? Which systems have been identified as GMP critical? | An up to date and if applicable a modular list is expected. This list should be a controlled document (record). A system description should be available for GMP critical systems. |
| 2.3.1.11 | What are the defined criteria for a system ranked as GMP critical? | A SOP or checklist (form) or a documented assessment on the basis of the SOP or a checklist for each system is expected. |
| <i>4.4 User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User requirements should be traceable throughout the life-cycle.</i> | | |
| 2.3.1.12 | User Requirements are the basis for validation activities. These should also be created for a retrospective validation ⁶ . The aim of validation is to proof that the system is capable to fulfil the requirements. The extent (range) of the user requirements depends on the complexity of the system. NOTE: A more risk-based approach would define the extent of the needed requirements on the complexity of the process – not to the system. | |
| 2.3.1.13 | Who created the User Requirements? | User Requirements should be created by the operator of the system. Also it is possible to analyse the functional specification of the supplier. |
| 2.3.1.14 | How are user requirements formulated / expressed? | User Requirement should be defined in order that these are checkable and verifiable. |

⁶ We totally disagree with this interpretation. It should not be mandatory to create an URS for an existing system, if there is an accurate process map, process risk assessment and up-to-date system description.

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 16 of original |
| Nonbinding translation by CCS | | ZLG |

2.3.1 Validation

| No. | Related Questions | Comments |
|--|---|--|
| 2.3.1.15 | How can the system be represented to show that it fulfils the requirements, especially critical user requirements? | It is expected that critical requirements are identified and that the validation process assures traceability and their successful coverage. During an inspection a verification of such critical requirements should be executed, in order to check consistency between different life cycle documents, e.g. Functional Specification, Risk Assessment, Test Report, etc. |
| 2.3.1.16 | Was a risk assessment on the basis of the user requirements executed? Which requirements were ranked as critical? | Refer to 3.3.1.15 |
| <i>4.5 The regulated user should take all reasonable steps, to ensure that the system has been developed in accordance with an appropriate quality management system. The supplier should be assessed appropriately.</i> | | |
| 2.3.1.17 | In general software is purchased and then particularly configured towards the own requirements (software category 4; according ISPE GAMP 5). Because of this the process of software development is executed by a third party and can not be under full control, the supplier evaluation and assessment has a extraordinary relevance to verify that the software is developed according quality assurance methods. | |
| 2.3.1.18 | Was the supplier evaluated / assessed? | An on-site audit is expected for critical systems close to production. Suppliers of less critical systems can be assessed by a postal audit. |
| 2.3.1.19 | Was a certification referenced for the assessment of the supplier? | If the supplier was certified according an adequate standard and this fact was considered for the supplier assessment, it is required to inquire if the product (software or hardware) was developed according the certified Quality System. |
| <i>4.6 For the validation of bespoke or customised computerised systems there should be a process in place that ensures the formal assessment and reporting of quality and performance measures for all the life-cycle stages of the system.</i> | | |
| 2.3.1.20 | Spread Sheet Applications are very often (extensively) used in the pharmaceutical industry. If so called VBA macros or SQL statements are integrated into such worksheets, these should be noted as Custom Build Systems (software category 5 acc. ISPE GAMP 5). | |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 17 of original |
| Nonbinding translation by CCS | | ZLG |

2.3.1 Validation

| No. | Related Questions | Comments |
|---|--|---|
| 2.3.1.21 | Which documents for custom build software have been created additionally compared to configurable standard software packages? | Custom Build Systems are developed especially for one single customer. On request (by the inspector) there should be a proof of actions regarding code review, unit testing, and integration testing. At least the corresponding reports should be available at the supplier and should be embedded into the supplier's quality system. The procedural method should have been assessed in the scope of the supplier audit. Databases are very often a matter of custom build or individual configured systems. |
| 2.3.1.22 | Where and how are configuration settings of a system documented? Are changes of configuration (items) traceable? Is it possible to trace / relate a specific configuration (setting) to its respective Software/Release (version)? | Customized Systems are specific configured according the requirements of the users. The configuration and the resulting functionality should be documented and should be verified by testing. <i>adequacy.</i> To each configuration (set) the corresponding Version / Release of Software should be documented. |
| <i>4.7 Evidence of appropriate test methods and test scenarios should be demonstrated. Particularly, system (process) parameter limits, data limits and error handling should be considered. Automated testing tools and test environments should have documented assessments for their adequacy.</i> | | |
| 2.3.1.23 | How was the adequacy of test cases proved? | The expected test result and the test execution can be derived from the test description. |
| 2.3.1.24 | How are critical data fields verified? | Especially if critical data are triggering follow-up actions, boundary values and other values (e.g. letters instead of numbers) should be used for testing purposes. |
| 2.3.1.25 | Are automated testing tools used? How was their adequacy assessed? | Critical functions of a test tool should be verified. The suitability of test data should be documented. |
| <i>4.8 If data are transferred to another data format or system, validation should include checks that data are not altered in value and/or meaning during this migration process.</i> | | |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 18 of original |
| Nonbinding translation by CCS | | ZLG |

2.3.1 Validation

| No. | Related Questions | Comments |
|-----------------|---|---|
| 2.3.1.26 | Due to software upgrades, a system change (replacement) or a system decommissioning it might be required, that existing data of a legacy system is migrated respectively transferred into another system. This is a critical proces requiring planning and testing. Especially different data formats (types) may have an impact on data integrity. Archiving of data is a form of migration. | |
| 2.3.1.27 | How is the sample amount for random sampling defined, which are used and verified during the migration process? | This is depending on the criticality of data (e.g. Blood databases or ref. FDA: Blood Establishment Computer Software - BECS , infection serological data). In any case all different (data) formats should be checked. Adequate statistical sample values can be derived from DIN ISO 2859 Part1. |
| 2.3.1.28 | Which strategy is followed for data migration? Which approach is in the migration plan described? | There should be a migration plan exiting. Tests of the data migration should be done in a test environment. It is important that migration data was checked according the criteria defined in the migration plan afore. It should be considered, that data can be migrated across diverse interfaces and with miscellaneous starting data formats. |
| 2.3.1.29 | How is it ensured that the meaning and units (of data) are correctly transferred? | During the migration (process) the units of measurements (e.g. g, kg) and the acceptance of values / data (as in infection serology) should not be changed or in case of changes correctly transferred. |
| 2.3.1.30 | Archiving of data may also be a migration to another storage media. It is desirable not to maintain a museum of old equipment and systems, so it is often necessary to migrate data and metadata. Metadata are information, which is required to interpret data, for example integration parameters. | |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 19 of original |
| Nonbinding translation by CCS | | ZLG |

2.4 Operational Phase

2.4.1 Data

5. Data - Annex 11

Computerised systems exchanging data electronically with other systems should include appropriate built-in checks for the correct and secure entry and processing of data, in order to minimize the risks.

2.4.1 Data

| seq. no. | Related Questions | Comments |
|----------|---|---|
| 2.4.1.1 | Nowadays systems are more and more interconnected to each other instead of standalone systems operated formerly. By transmitting data (electronically) from one system to another the error source of incorrect (manual) inputs is reduced, but such (systems') interfaces should be investigated during validation in detail. Because interfaces are parts of both systems (connected to each other), it should be considered that a change at one system may have an impact on such an interface and hence resulting into follow-up changes to the other system. | |
| 2.4.1.2 | We distinguish between unidirectional and bidirectional interfaces. Unidirectional interfaces are transmitting data only into one single direction (between source and target system); bidirectional interfaces into both directions. | |
| 2.4.1.3 | Between which systems are data transferred? Which systems are exchanging data between each other? Which protocols are used? | Based on the criticality of the systems it can be decided during an inspection, if a detailed verification is required. |
| 2.4.1.4 | Which technical protocols are used for the data transfer? | If a (simple) "transport" of data is carried out merely on one single direction (connection) and a standard protocol (e.g. TCP/IP) is used, this is generally not critical. However if different data formats are existing on each of the systems, changes to the data at the interface (gateway) will happen. Examples for different formats: Date format DDMMYYYY - MMDDYY. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 20 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.1 Data

| seq. no. | Related Questions | Comments |
|----------------|---|---|
| 2.4.1.5 | At which interfaces are data converted? | Among changes of the units of measurements (e.g. g instead of kg) changes of the data format are also possible (e.g. comma or decimal point as decimal separator). This should be specified and tested. |

2.4.2 Accuracy Checks

6. Accuracy Checks - Annex 11

For critical data entered manually, there should be an additional check on the accuracy of the 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 covered by risk management.

2.4.2 Accuracy Checks

| No. | Related Questions | Comments |
|----------------|--|--|
| 2.4.2.1 | Which data (sets) have been identified by the risk analysis as critical? | It should be pre-defined, which data sets are ranked as critical ones. In principle companies are free to define which data is ranked as critical. However values (data), which are used for the rejection or approval of API, semi-finished, or final product batch, should be seen as critical data during an inspection. |
| 2.4.2.2 | Where is manual data entry (input) done? | Manual data inputs is error-prone. During an inspection it should be looked out to where data is entered manually. For example the entry of a batch number or of the expiry date for packaging processes should be noted, or the input of boundary values for an belt weigher / scales. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 21 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.2 Accuracy Checks

| No. | Related Questions | Comments |
|----------------|--|--|
| 2.4.2.3 | How and who is performing an additional verification / review? | <p>According Annex 11 such verifications can be done by a second operator – requiring a prompt verification – or by a validated, electronic method.</p> <p>As an electronic method it is for example imaginable that an error checking number for numeric values (existing for the central pharmaceutical number or for many barcodes), the display of error messages, if boundary values are exceeded, or even plausibility checks, if an operator must enter several values (e.g. Product Number, Batch, Amount), and the system is comparing the „fitting correlation“ with values of the database.</p> |
| 2.4.2.4 | Which follow-ups / consequences do have a faulty data entry? | The consequence of a faulty manual data input should be assessed. Based on the impact level there should be appropriate control measurements implemented. |
| 2.4.2.5 | Which additional tests covering faulty inputs are available? | <p>For example at a belt weigher for packaging: Wrong entries of boundary values may cause that missing blisters are not detectable. If before production start a proof with an dummy package is executed, the faulty entry can be detected immediately, and consequently a correction of the wrong entered data can be executed.</p> <p>It is also imaginable, that a faulty data entry (e.g. correction factor) causes a deviation of the yield or stability.</p> <p>For critical data an additional verification is mandatory.</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 22 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.2 Accuracy Checks

| No. | Related Questions | Comments |
|----------------|--|--|
| 2.4.2.6 | <p>What kind of accuracy checks are performed for „Excel“ spreadsheets?</p> <p>Note: Inspectors are also using the common speech to call Spreadsheet Applications simply as “Excel” (product name). It is applicable for all available spreadsheet applications.</p> | <p>If Spreadsheet Applications are used for calculations or statistics/analysis, it should be considered, that so called templates are used. These can be identified by the file extensions of „.xlt“ respectively „.xltx“⁷. The re-use of worksheets, which have been also used previously and still containing values, should be complained during an inspection, because of the risk of using values from the previous analysis.</p> <p>Such templates should be managed as controlled documents similar to Processing Instructions or Batch Processing Record, and should be version controlled and under change control process.</p> |

⁷ This is a nice and simple explanation, but not mandatory, if for example templates are managed by an electronic document management system. The intention is to assure the usage of the correct templates.

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 23 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.3 Data Storage

7. Data Storage - Annex 11

7.1 Data should be secured by both physical and electronic means against damage. Stored data should be checked for accessibility, readability and accuracy. Access to data should be ensured throughout the retention period.

7.2 Regular back-ups of all relevant data should be done. Integrity and accuracy of back-up data and the ability to restore the data should be checked during validation and monitored periodically.

| 2.4.3 Data Storage | | |
|---------------------------|--------------------------|--|
| No. | Related Questions | Comments |
| 2.4.3.1 | | <p>It is important to differentiate between Data Storage and Archiving.</p> <p>For Data Storages there is a difference between incremental and full back-ups. A full back is a copy of all data sets dedicated to the entire data storage.</p> <p>For an incremental back-up, after an initial full back-up, only data sets are copied, which have been modified since the last back-up. The advantage is, that less storage (disk) space is required and the backup can be executed faster; the disadvantage is that for a data recovery the last full full-back needs to be imported first and then subsequently all incremental back-ups (stepwise).</p> |
| 2.4.3.2 | | <p>The term generation is defining the amount of the saved data storages, before starting the re-write of the data storage media. Very often several overlapping generations can be found. For example the daily data storage is run from Monday to Thursday on one single storage media. Friday's back-up is run as a weekly storage, and for example for 4 weeks stored and from the ones of the first Fridays in each month the last six backups (monthly / half-year backups).</p> |
| 2.4.3.3 | | <p>RAID stands for: „Redundant Array of Independent Disks“.</p> <p>Commonly used in the pharmaceutical industry are RAID 1 and RAID 5:</p> <p>RAID 1 (Mirroring) – Data is stored on two independent data storage volumes – it is not acceptable for replacing data storages and backups, because errors like deletions are also mirrored.</p> <p>RAID 5 (Block-level striping with distributed parity) – Data is distributed at a minimum of 3 storage volumes. By the information of parity saved at one volume as data sets, the data can be reconstructed from the other volume in the case of the outage of any other storage volume.</p> <p>RAID-systems are a part of data availability and a protection of data loss caused by defect storage volumes. However RAIDs are not appropriate for the process of data storage, because deletions or accidental modifications are impacting always also the redundantly stored data.</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 24 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.3 Data Storage | | |
|---------------------------|--|---|
| No. | Related Questions | Comments |
| 2.4.3.4 | Which procedure (method) is used for data storage? How often is data backed up? | <p>In any case data storage is required. The frequency of data storages can be very different. As an indication for the necessity of backups the frequency of data input or changes can be used.</p> <p>For example: A system for the recording of the critical environmental parameters may be stored on a hourly basis, contrary on a weekly basis the disc drive locations of SOPs.</p> |
| 2.4.3.5 | How many generations of data back-ups are stored? | <p>Typically more then one data backup is stored. The current method is to store data for each weekday one separate storage volumes/media and to re-write them after one week. Very often additional weekly and/or monthly backups are created. There are also systems available which provide a history over a longer period (e.g. hourly for the past 24 h, daily for the past month, and weekly for the last months).</p> |
| 2.4.3.6 | Is the process of data recovery validated? | <p>In any case the recovery process of the data storage should be tested.</p> <p>For complex systems the data recovery will not be executed on the so called productive system (environment). At such complex systems a so called three-system-landscape can be found very often; existing of a development, test and productive system. In this case it is acceptable when the data recovery is tested on the test system.</p> |
| 2.4.3.7 | Where is the storage location/area (physically) of the storage volumes / media? | <p>At least the storage media should be stored in a separate fire zone (e.g. separate fire zone to the server room/data center).</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 25 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.4 Printouts

| |
|--|
| 8. Printouts - Annex 11 |
| <i>8.1 It should be possible to obtain clear printed copies of electronically stored data.</i> |
| <i>8.2 For records supporting batch release it should be possible to generate printouts indicating if any of the data has been changed since the original entry.</i> |

| 2.4.4 Printouts | | |
|-----------------|--|---|
| No. | Related Questions | Comments |
| 2.4.4.1 | According Chapter 4 ⁸ (EU GMP Guide) regulated users should define for electronic data which data are to be used as raw data. At least, all data on which quality decisions are based should be defined as raw data (original text of chapter 4). | |
| 2.4.4.2 | Which data is printable? | All data defined as raw data and all information required for the interpretation of such data (metadata) should be printable. |
| 2.4.4.3 | Are post-changes observable a) at the display screen? b) on the print-outs? | <p>Basis of this requirement is § 10 Chapter 1 AMWHV (German Ordinance on Manufacturing of Medicinal Products and Active Ingredients) and Annex 11 No. 8.2.</p> <p>Changes of critical data should be documented by audit trail. Before batch release any post-changes of quality data should be verified. Especially for electronic documentation such changes are not automatically detectable or visible. For example it is sufficient if changes or modifications are visible by underlined data (text), in order to simply detect the changed value and to investigate the original value located in a log-file.</p> <p>If during an inspection such changes are observable on the screen, the related print-out can be asked for, in order to verify the print-out against the visibility of the displayed changes on the screen.</p> |

⁸ Note: Reading Annex 11 without Chapter 4 in parallel is imperfect. Compliance to Annex 11 requires at minimum the full understanding of Chapter 4.

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 26 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.4 Printouts

| No. | Related Questions | Comments |
|----------------|---|---|
| 2.4.4.4 | Which procedures are in place, if such functionality is not yet available? (Note: refer to No. 2.4.4.3 – function in the meaning of printing raw data and meta data) | If the system was installed before July 2011 (effective date of Annex 11 – Revision 1) and does not provide such functionality, it might be exceptionally acceptable, if an analysis of the audit trail is executed and the results are documented before a batch release, defined by an corresponding SOP. |

2.4.5 Audit Trails

9. Audit Trails - Annex 11


Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

2.4.5 Audit Trails

| seq. no. | Related Questions | Comments |
|--|--|--|
| <i>Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail").</i> | | |
| 2.4.5.1 | Which processes are GMP-relevant? | In general GMP relevant processes are described in the User Requirement Specification. The methodology of the risk assessment for the classification of GMP-relevant and non-GMP-relevant processes should be adequate. |
| 2.4.5.2 | Which input fields do contain critical data? | It is not required that all data fields of an GMP-relevant process are under Audit Trail. A detailed risk assessment should result into a determination of the factual critical and process-relevant data. Critical parameters (variables) / values should be covered by the Audit Trail. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 27 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.5 Audit Trails | | |
|---|---|---|
| seq. no. | Related Questions | Comments |
| 2.4.5.3 | When are audit trails deleted? | It is not allowed to change or to delete in principle Audit Trails (records). If the retention period of the data sets is expired, the corresponding Audit Trail data can also be deleted. It should be challenged, how it is assured that only the corresponding audit trail data will be deleted. |
| <i>For change or deletion of GMP-relevant data the reason should be documented.</i> | | |
| 2.4.5.4 | This is a new requirement and should assure that changes or deletions of data are traceable. | |
| 2.4.5.5 | Who is allowed to change or delete data? | The authorisation for changing/deleting data should be defined in the user / role concept. A unique user identification and date & time stamp (designation) is required. |
| 2.4.5.6 | How is the rational/ justification of a change or deletion (electronically) documented? | The rational can be given in form of a free text. Drop-/Pull-down-menus are also acceptable. In any case the given rational should be reproducible in form and content. The input of the rational (reason for change or deletion) should be mandatory forced by the system. |
| <i>Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.</i> | | |
| 2.4.5.7 | Which information is recorded in case of changes and deletions? | At least following information should be available: <ul style="list-style-type: none"> - „Who“, „What“, „When“ and „How“ changed it, - Display of the original (initial) value(s) and of the changed value. - Reason for change or deletion |
| 2.4.5.8 | How often are Audit Trails checked periodically? | One the one hand the functionality of the audit trail and on the other hand data sets of the audit trail should be verified. The time periods should be reasonable and should be defined according the process risks. |

| | | |
|----------------------------------|--|---|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 28 of original |
| Nonbinding translation by CCS | |  |

| 2.4.5 Audit Trails | | |
|---------------------------|--|--|
| seq. no. | Related Questions | Comments |
| 2.4.5.9 | What actions have been taken for „legacy systems“ which do not provide an Audit Trail functionality for changes and deletions? | <p>Legacy Systems are systems, which have been installed before Annex 11 (1992) was effective.</p> <p>In the first instance it should be investigated, if data can be changed at all (e.g. electronic chart recorder). If not (changeable), there is no need for an Audit Trail.</p> <p>For systems without an Audit Trail functionality it can for example be stipulated by an SOP, that every change needs to be recorded into a logbook and verified by a second person.</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 29 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.6 Change and Configuration Management

10. Change and Configuration Management - Annex 11

Any changes to a computerised system including system configurations should only be made in a controlled manner in accordance with a defined procedure.

| 2.4.6 Change and Configuration Management | | |
|--|--|--|
| seq. no. | Related Questions | Comments |
| 2.4.6.1 | When will changes recorded and implemented? (from which point of time) | Changes should already be recorded and assessed during the development phase. Such changes might potentially impact also the User Requirement Specification or Functional Specification. The transition from the development phase to the operational phase should be clearly defined. It might be required to establish two different procedural workflows. |
| 2.4.6.2 | Which elements (topics) are covered by the change management? | Commonly accepted: <ul style="list-style-type: none"> - Definition of roles (e.g. request, assessment, actions, execution, closure), - Method of documentation, - Request incl. reason, - Evaluation of GMP-relevance and process risk, - Defined actions and testing, - (Pre-)Approval, - Execution, - Conclusion (Post-Approval) and feedback to change initiator. The category and criticality of the change may have an impact on the required actions / steps (workflow, documentation). Repair activities like replacements of similar components may be defined as pre-approved change activities. |
| 2.4.6.3 | Which elements (items) are defined for configuration management? | Commonly accepted: <ul style="list-style-type: none"> - Method of documentation, - Programming/ parameterization (customization or configuration). |
| 2.4.6.4 | How are changes categorized? | At least the classification should be defined to the category "GMP-relevant" and "not GMP-relevant". Additionally it is recommended to classify a change to "critical" and "noncritical". A reduction / cutback of actions (validation yes/no and validation scope) is only possible on such a basis. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 30 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.6 Change and Configuration Management

| seq. no. | Related Questions | Comments |
|----------------|---|---|
| 2.4.6.5 | Which controls are in place for changes of the configuration? | Such controls should be defined system-specific; Actions should be defined on the basis of a risk assessment. |

2.4.7 Periodic evaluation

11. Periodic evaluation - Annex 11

Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.

2.4.7 Periodic evaluation

| No. | Related Questions | Comments |
|---|--|---|
| <i>Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP.</i> | | |
| 2.4.7.1 | How often are periodic evaluations performed? | Annex 11 is not defining a period/ interval. The periods should be defined by the pharmaceutical company. For different systems different intervals can be defined. At a minimum evaluations should be done on an annual basis. Other periods should be reasonably founded. The scope and method of a periodic evaluation should be defined in written form (documented). According the GMP-relevance and criticality a corresponding categorization can also be applied. |
| <i>Such evaluations should include, where appropriate, the current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.</i> | | |
| 2.4.7.2 | Who is responsible for the execution of the period evaluation? | There are no (regulatory) requirements existing. There should be a definition of a precise commitment, who is responsible for the execution and who might be delegated for the execution. The evaluation should be done in cooperation with all involved departments/units (QA, IT, operational departments etc..). |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 31 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.7 Periodic evaluation

| No. | Related Questions | Comments |
|----------------|--|---|
| 2.4.7.3 | Is the evaluation delegated (out-sourced) to a service provider (3 rd party)? | <p>The task/execution can be delegated, but not the responsibility.</p> <p>Possible Responsibilities: QA or system owner, production / quality assurance or validation team/unit – ultimately the pharmaceutical company is responsible, respectively the Qualified Person.</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 32 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.8 Security

| |
|--|
| 12. Security - Annex 11 |
| <i>12.1 Physical and/or logical controls should be in place to restrict access to computerised system 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.</i> |
| <i>12.2 The extent of security controls depends on the criticality of the computerised system.</i> |
| <i>12.3 Creation, change, and cancellation of access authorisations should be recorded.</i> |
| <i>12.4 Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.</i> |

| 2.4.8 Security | | |
|-----------------------|--------------------------|---|
| No. | Related Questions | Comments |
| 2.4.8.1 | | For the improvements of computerized systems' security several actions should be considered, for example data storage, controlled data access, data encryption, virus protection, usage of firewalls. The selection of the actions are depending on the criticality of systems and data. |
| 2.4.8.2 | | The assignment of access rights to company-internal employees should assure, that personnel is getting access to data and programmes in order to fulfil their delegated tasks (responsibilities). |
| 2.4.8.3 | | There are several possibilities depending on the operating systems. If system access is granted to several persons, the authorisation to files and programmes should be defined accordingly. It should be noted, that there might be several levels for the access assignments. For example, it is possible to assign access rights to one file or program only to one single user. However it is also possible to assign access rights to predefined groups (e.g. supervisor) or to all users of a system. |
| 2.4.8.4 | | As far as access rights are assigned to user groups, a check during the inspection can be performed to verify such group settings and the individual persons assigned to such groups. The assignment of access rights to groups is only exceptionally acceptable, e.g. read-only access rights. |
| 2.4.8.5 | | If during an inspection a verbal description of the required access rights of a group is given, it can be verified, if the individual persons do have the required access rights to fulfil their duties. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 33 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.8 Security | | |
|-----------------------|--|--|
| No. | Related Questions | Comments |
| 2.4.8.6 | A conceptional enhancement is given through the access rights management by providing user roles (short: roles) for user groups. Such a role defines tasks, properties, and particularly user access rights (or administrator rights) for a software or an operating system. Instead of assigning rights directly to single users or groups, a (generic) role is pre-defined and users are assigned to it. This implies that a single user can be assigned to several roles. This is a simplified method for the access rights management. | |
| 2.4.8.7 | How are abortive access attempt documented? | Such documentation can be assessed during an inspection. The documentation should contain by which user ID, date and time, and location the access attempt was done. For example in such a case and if a significant occurrence is detectable it can be asked what kind of actions have been defined/taken. After several abortive attempts for the access to the computerized system (e.g. wrong password), the respective access should be blocked. A procedure for "unblocking" should be available. |
| 2.4.8.8 | What kind of actions are defined for the protection of external influences (e.g. virus)? | If external data from the internet (network) or from memory mediums are downloaded and opened, the implementation and usage of antivirus software is mandatory. Systems which are connected over the internet should be protected by a suitable firewall. In addition several internal networks may require firewalls for the protection of nearby networks. Antivirus and Firewall software should be updated on a regular basis. |
| 2.4.8.9 | Who is assigning access rights and how is the process defined? | The roles and authority of administrators should clearly be defined. Administrators should be trained accordingly to their duties. |
| 2.4.8.10 | What kind of provisions were defined to assure usage of safe passwords? | There should be guidelines defined for passwords covering the length, used symbols/characters, period of validity, and their reuse. A common standard can be found at the Federal Office for Information Security - BSI (German: BSI IT- Grundschutz): Password must be at least 7 characters long, passwords do not match dictionary words or names, and should contain special and numeric characters. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 34 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.8 Security | | |
|---|---|--|
| No. | Related Questions | Comments |
| 2.4.8.11 | Who is allowed to change data (and when)? | Permissions should be restricted to defined persons by name. This applies to “ <u>confirmed</u> data <u>inputs</u> “ only. If during the data entry a user mistypes a value and performs an immediate correction, this is not defined / interpreted as a change in the context of Annex 11. Right after the confirmation (in many cases with the Enter-/Return key) and saving the data set, from this point forward it is seen as a change according Annex 11. |
| 2.4.8.12 | How are these permissions regarding data inputs and changes recorded? | Permissions should be properly recorded in order to be able to investigate which user had what permissions at what time period granted or lost. It is important to check, who is allowed to make changes and if the requirements of the German AMWHV (subsequent recognisability) is fulfilled. |
| <p><i>12.1 Physical and/or logical controls should be in place to restrict access to computerised system 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.</i></p> | | |
| 2.4.8.13 | Which methods are used to avoid system access for not authorized persons? | It is important to distinguish between: <ul style="list-style-type: none"> - physical access control (rooms) and - logical access control/authorization (software). Both aspects should be considered during an inspection. The system should have the ability to identify tasks for each individual user (e.g. by linking user ID and password to a unique combination, from which an authorisation for a special application is derived). |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 35 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.8 Security | | |
|---|--|---|
| No. | Related Questions | Comments |
| 2.4.8.14 | Which persons are allowed to change data? | Data inputs and changes are allowed only by persons, which are properly assigned and trained: - Data input: Only by persons, who are dedicated to the system by a description of the work center (operator's position). - Changes: by the function owner according the German Medicines Act (AMG/AMWHV) or a delegated person by him/her. |
| 2.4.8.15 | Which rules are defined for the assignments of access rights? | The assignment of access rights should be defined by a SOP. Generally the assignment of rights to a network respectively for signatures should be separated between different roles (<i>in the meaning of avoiding exclusive rights by an individual</i>). |
| 2.4.8.16 | How is the system verifying the user's identity, who is entering, changing, or confirming critical data? | The identification of a user can be done by: a) Knowledge, e.g. User ID and password b) Ownership, e.g. smartcard, key, c) Biometric, e.g. finger print, voice, face. Commonly used is variant a). For security-relevant areas is variant b) used. Nowadays biometric identification is still in an unusual manner. Validation of such systems should be critically scrutinized. |
| <i>12.3 Creation, change, and cancellation of access authorisations should be recorded.</i> | | |
| 2.4.8.17 | Which processes / procedures are in place for the creation, change, and cancellation of access authorisations regarding data inputs and changes? | Granting of appropriate access rights should be limited to the user's assigned scope of work. Within the exit process or in case of an operational change by an employee the (formerly assigned) access rights should be deactivated. It should be checked (<i>during an inspection</i>), if the access rights assigned in the system coincide with the given statements of an employee. An index (list) of authorized persons should be maintained. |
| 2.4.8.18 | How is the procedure described in terms of data entries and changes? | For this point the inspector's team can verify, if actually only authorized persons have access to enter and change <i>data/permissions</i> . |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 36 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.9 Incident Management

13. Incident Management - Annex 11

All incidents, not only system failures and data errors, should be reported and assessed. The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.

2.4.9 Incident Management

| No. | Related Questions | Comments |
|---|---|---|
| <i>All incidents, not only system failures and data errors, should be reported and assessed</i> | | |
| 2.4.9.1 | What is the definition of an incident? | A company can define, what an incident and an intended use (specified normal operations) means. For example the activity of resetting an password is a normal operation and is not an incident case, because the system is also recording it by a log-file. |
| <i>The root cause of a critical incident should be identified and should form the basis of corrective and preventive actions.</i> | | |
| 2.4.9.2 | How is the classification of incidents defined? | At least there should be a determination of critical and noncritical incidents. The root cause should be documented and corrective and preventive actions should be defined. Based on the incident category different workflows for incident handling may exist. |
| 2.4.9.3 | Who is involved in the incident process? | It should be defined by an SOP who is recording and working on an incident case. Roles and functions should be defined for the logging, assessment, defining actions, the final conclusion and follow-up actions. According to the criticality level the process owner and under certain conditions the Qualified Person / QA should be involved. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 37 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.10 Electronic Signature

14. Electronic Signature - Annex 11

| |
|--|
| <p><i>Electronic records may be signed electronically.</i></p> <p><i>Electronic signatures are expected to:</i></p> <p><i>a. have the same impact as hand-written signatures within the boundaries of the company,</i></p> <p><i>b. be permanently linked to their respective record,</i></p> <p><i>c. include the time and date that they were applied.</i></p> |
|--|

| 2.4.10 Electronic Signature | | |
|-----------------------------|---|---|
| No. | Related Questions | Comments |
| 2.4.10.1 | It is the field of direct responsibility of the regulated company to define the usage and methods/class of electronic signatures instead of handwritten signatures. Legally binding GMP-requirements for the type and quality grade of an electronic signature are not existing. The (German) Digital Signature Act is not applicable. Therefore, in the scope of an inspection of electronic signatures, it is initially important to know the company's internal definition for the approval of documents, particularly with regard to permissions and access right concepts. | |
| 2.4.10.2 | The meaning of an electronic signature should be defined identically by the company according GMP-requirements as for handwritten signatures; this does not require an extra (special) mention in Annex 11. | |
| 2.4.10.3 | Which documents are signed electronically? | This question helps to get an overview of electronically signed documents, also with regard to the criticality of the electronic signature. |
| 2.4.10.4 | Which type(s) of electronic signatures are used? | The type of an electronic signature is not legally prescribed (see above). For the cases, that electronic signatures are used on batch processing records, test specifications, or batch release documentation (ref. EU GMP Chapter 4 - Manufacturing Formulae, Processing, Packaging and Testing Instructions, CofA and Reports), the usage of an <i>advanced electronic signature</i> is recommended (refer to ZLG Votum V11003 – available in German language only). If “simple” electronic signatures are used, the evidence of indisputability is of major significance. The minimum requirement for the execution of an electronic signature is to reapply (re-enter) the password. A simple functional button or a generated display of a name by command does not represent an electronic signature. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 38 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.10 Electronic Signature | | |
|------------------------------------|---|--|
| No. | Related Questions | Comments |
| 2.4.10.5 | Do approvals exist on electronic documents, which were not signed electronically? | Potentially documents are in place, which are released or approved by a simple functional button (key) or a user command (for example within an electronic workflow). For such cases this is not (seen as) an electronic signature and it should be verified, if the equivalent / notional paper-based version would be sufficiently represented by given initials. In any case the system should record the user's identity, who reviews, edits, approves or releases such documents. |
| 2.4.10.6 | Is there a written confirmation letter existing by the persons using electronic signatures, in order to accept electronic signatures as the equivalently legal binding to hand-written signatures within the boundaries of the company? | Because Annex 11 is merely focusing on the inner relationship (within the boundaries of the company), such a written confirmation (declaration) should be in place – except that solely qualified electronic signatures according to the e-Signature Act are used – in order to make the authenticity of the signature undeniable / undisputable. |
| 2.4.10.7 | Is a subsequent change of an electronically signed document possible? If yes, is the change cognizable? Is the signature still valid? | It must be assured that subsequent changes of already signed documents are cognizable and the previous given signature becomes invalid because of the change. |
| 2.4.10.8 | How is the identity of an operator checked? | In general the identity is verified by user ID and password; requiring a corresponding access rights concept (see No. 2.4.8 – reference corrected - and Annex 11 – sec. 12). Alternative solutions like token cards or keys are also acceptable. The validation of systems using biometrics should be challenged in detail. |
| 2.4.10.9 | How were the principles of the electronic signature and the indelible linkage between the electronic signature and the signed document validated? | The identical conditions do apply as for the validation of other systems. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 39 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.10 Electronic Signature

| No. | Related Questions | Comments |
|------------------|--|--|
| 2.4.10.10 | Are electronically signed documents transferred by interfaces to other systems or are any workflows started by an electronic signature? | In order to find out, if other systems are related to the focus of the inspection, it should be questioned, if interfaces to other systems or processes exist. |
| 2.4.10.11 | How long are electronically signed documents stored? Are electronically signed documents migrated to other systems respectively to archive systems? | The retention period is identically for electronically signed documents to hand-written signed documents. If electronically signed documents are archived or migrated, refer to 2.3.1 (Annex 11 chapter 4.8) and 2.4.13 (Annex 11 chapter 17). |

2.4.11 Batch release

15. Batch release - Annex 11

When a computerised system is used for recording certification and batch release, the system should allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.

2.4.11 Batch release

| No. | Related Questions | Comments |
|-----------------|--|--|
| 2.4.11.1 | If the certification of the batch release is done electronically, Annex 11 (solely mandatory at this place) requires an electronic signature. | |
| 2.4.11.2 | The certification of a batch release should be seen in contrast to any further activities, for example the execution of a status change of a certified finished product batch. | |
| 2.4.11.3 | How is the electronic certification carried out? | At this point it is recommended to ask for a live demonstration of the electronic signature process. It should be verified, if it is actually an electronic signature (per definition) and that only the Qualified Person can perform the signature exclusively. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 40 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.11 Batch Release

| No. | Related Questions | Comments |
|-----------------|---|---|
| 2.4.11.4 | Are automated interfaces in place to other systems? Are batch release information manually processed? | After the electronic certification of the batch release it should be recorded into the batch index (register), afterwards the release decision can be executed, for example by a status change of the pharmaceutical product. Depending on, if it is done manually or by automated interfaces between systems, the requirements according 2.4.1 and 2.4.2 (chapter 5 and 6 Annex 11) should be considered. |
| 2.4.11.5 | Are automated data collections used in the context of the release process? | <p>Provided that individual data collections are created, such systems should be entirely validated.</p> <p>Collected data (summaries), which might be provided by production equipment (e.g. tablet press, sterilizing tunnels), are normally qualified. However individual parameterisation (recipes/formula) should be checked separately.</p> <p>Note: For qualification there is also a Aide Memoire of the ZLG existing (# 07121105).</p> |
| 2.4.11.6 | Are changes to release-relevant data detectable by the Qualified Person? | Special attention should be paid to changed data (e.g. in the context of OOS and deviations), that such changes are clearly detectable for the Qualified Person. The Qualified Person should be able to create / obtain meaningful print-outs. |
| 2.4.11.7 | Does the Qualified Person have access to all relevant data before the release decision? | The requirements of Chapter 4 of the EU GMP Guideline do apply also to the case of batch releases with electronic systems. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 41 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.12 Business Continuity

| | | |
|--|--|---|
| 16. Business Continuity - Annex 11 | | |
| <i>For the availability of computerised systems supporting critical 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 based on risk and appropriate for a particular system and the business process it supports. These arrangements should be adequately documented and tested.</i> | | |
| 2.4.12 Business Continuity | | |
| No. | Related Questions | Comments |
| 2.4.12.1 | Critical processes should be identified and listed/registered. | |
| 2.4.12.2 | Examples for possible breakdown scenario are (remedial measures given in brackets) are: <ul style="list-style-type: none"> - Outage of components, e.g. printer or scales (keep spare parts in store), - Current fluctuation or electrical power outage (compensation systems or emergency power supply), - Damage on hardware by external influences (provision of spare systems), - Abnormal system end / breakdown (local data buffer), - Virus attack or similar (continuous updating of anti-virus software). | |
| 2.4.12.3 | Number 16 of Annex 11 is not limited only to batches currently processed in the production process, but also to batches in-use / in circulation (e.g. for recalls). Because of this it should be pre-defined for time-critical processes, in which time period alternative actions should be in place / up and running. | |
| 2.4.12.4 | Is an action plan in place and how is it structured? | The content of an action plan should include: <ul style="list-style-type: none"> - Description of possible failures and situations with indication of likelihood and frequency of occurrence. - Explanation of alternative systems available, if applicable, - Process description in case of failures and outage situations, - Instructions for the required documentation and if applicable maintenance of alternatively recorded data into the computerized system, - Description of the boot up process of the computerized systems after bug fixing. - Naming of authorized persons for the recommissioning (process). <p>The action plan should be reviewed on a regular basis; the responsible persons should be defined.</p> |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 42 of original |
| Nonbinding translation by CCS | | ZLG |

| 2.4.12 Business Continuity | | |
|-----------------------------------|---|---|
| No. | Related Questions | Comments |
| 2.4.12.5 | Is there a reporting procedure and what is the content? | <p>The reporting procedure should contain:</p> <ul style="list-style-type: none"> - Error / fault classification or description of disaster situation with impacts on the related process, - Determination of responsible persons for corrective actions, trouble shooting, error diagnostics and preventive actions. |
| 2.4.12.6 | What characteristics does have alternative procedures? | <p>The time frame of alternative processes replacing the failed processes, should be reasonable in terms of the related priority.</p> <p>Such alternative processes (procedures) should be in written form, should be validated and should be periodically verified related to correct functioning and promptly implementation/start-up.</p> <p>If data of the alternative process will be re-entered into the (initial) system, these data should be verified.</p> |
| 2.4.12.7 | How is the handling of recovered data defined in case of a power breakdown or other failures? | Data integrity and accurateness should be verified. |

| | | |
|----------------------------------|--|--------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 43 of original |
| Nonbinding translation by CCS | | ZLG |

2.4.13 Archiving

17. Archiving - Annex 11

Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

2.4.13 Archiving

| No. | Related Questions | Comments |
|----------|--|---|
| 2.4.13.1 | Important is the difference between backup and archiving. | |
| 2.4.13.2 | What tests are carried out to ensure the availability of the data? | <p>Storage disks have limited stability. Unfortunately, there are no binding reference data on the durability of electronic media. However the company should have made a determination internally, after which time the readability of archived data should be checked.</p> <p>Particularly when retention periods of more than six years are expected, it can be assumed that the data must be copied.</p> <p>It can also be assumed that for any length of retention periods hardware, operating systems, and applications may be changed. In such cases it should be verified if before shutdown of the previous system the data is accurately readable and not editable in the new system.</p> |
| 2.4.13.3 | Are disk media stored in a suitable place? | The durability of disk mediums also depends on environmental conditions. During inspections it can be for instance verified, if the storage recommendations of the media vendor are applied and if defined parameters (e.g. temperature) are monitored. |
| 2.4.13.4 | Which tests are executed, when data mediums are copied? | <p>As a minimum requirement a so called "verify" should be executed (in the meaning of a data check), which contains a comparison of both applications and/or data mediums.</p> <p>If it is not a copy to an identical storage medium, it should be questioned, if data is actually copied one-to-one (biunique) or if a change of data and its relations is rendered.</p> |

| | | |
|----------------------------------|--|--------------------------------------|
| Aide-mémoire 07121202 | Inspections of computerized systems | Page 44 to 49 of original |
| Nonbinding translation by CCS | | ZLG |

3 Definitions and abbreviations

This chapter was not translated.

It contains the full glossary of Annex 11 (original in English language – refer to http://ec.europa.eu/health/files/eudralex/vol-4/annex11_01-2011_en.pdf) and some additional definitions by the ZLG, refer also to <https://www.zlg.de/arsneimittel/deutschland/glossar.html>.

4 Attachments and Forms

Attachment 1 – Software Categories according GAMP5®

This chapter was not translated. It contains the identical definitions as given by ISPE GAMP 5. Attachment 2 is referencing to the German translation of Annex 11.

Chapter 5 (Reason of Change) and Chapter 6 (Further Reading) were also not translated. It should be noted that inspectors can access ISPE GAMP 5 through the PIC/S member area. It is not defined, if it contains also the ISPE Good Practice Guides.

END OF TRANSLATION

nonbinding translation by CCS

www.comes-services.com

contact us at: talk@comes-services.com