On January 3rd, 2011 the European Commission has published a **risk based approach** on computerised systems in GMP environments, the new

Annex 11 Computerised Systems

as part of the

The Rules Governing Medicinal Products in the European Union
Volume 4
Good Manufacturing Practice
Medicinal Products for Human and Veterinary Use

annex11_01-2011

The deadline for coming **into operation is 30 June 2011**.
By and large this annex 11 may be viewed as an equivalent to the US FDA 21 CFR 11 21CFR11.

The new European 4 page document is considerably more detailed than the current annex 11 anx11 with hardly 2 pages but much less voluminous than the intensively discussed draft from 2008 with 8 pages (annex_11_consult_200804.) Please refer to the attached table 3 for a comparison of the current annex 11, the 2008 draft and the annex 11-01-2011.

The annex 11-01-2011is subdivided in 5 chapters:
Principles
General
Project Phase
Operational Phase
Glossary
with a total of 17 numbered sections.

Take 5 minutes to playfully check your knowledge on annex 11-01-2011:

Annex11CheckYourKnowledge_v05.xlsm

Request a free copy of the check from PharmAdvice available as a macro enhanced Excel file recording and evaluating your answers and indicating in colour what's right or wrong and telling you why. Preview the 17 questions at the bottom of this text.

The following consideration summarize the new annex 11 requirements and correlate them with related GMP regulations

Whereas the basic idea of the annex ***"Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance." i***s almost literally transferred from the current annex 11 the emphasize on a ***risk management*** and a **risk based approach is more prominent** and **much more demanding** in the new annex 11. While the word "risk" is used only once in the current annex it appears 12 times in the new version, exactly 11 times in the annex text (please refer to table 1 below) and – by coincidence – one more time in the header of the document.

On one hand the ***documented risk assessment*** demanded by the annex offers the chance to tailor validation efforts exactly to each individual ***application***, on the other hand it is challenging to industry to keep all the risk assessments up to date. The regulated user needs to establish a process which links ***change control, periodic evaluation***, the ***inventory of the relevant systems and risk assessments***. PharmAdvice recommends creating and maintaining a controlled ***inventory*** file listing not only the ***relevant systems*** and their ***GMP functionality*** as required by chapter 4.3 but including all associated system life cycle documents and the date of their last review. Depending on the amount of systems to be monitored this may be a sophisticated database or a spreadsheet with appropriate protection against unintentional changes in the listing. Furthermore PharmAdvice recommends to include not only the ***relevant systems*** but also to include – as far as reasonable - those systems which have been rated "not GxP relevant" by the regulated user. The reason for that decision should also be included. PharmAdvice also strongly recommends considering end user applications like MS Excel ® spreadsheets and MS Access ® databases, because "*End User applications tend to be among the most under-documented systems used in GxP environments*[i]*".* This approach capturing all computerised systems has two advantages. In the first place it ensures that validation of GMP-relevant systems will not be overlooked and secondly the reasons not to validate are clearly stated and comprehensible to everybody. PharmAdvice admits, that this recommendation is very close to the wording of the 2008 draft *"An inventory, or listing, of all computerised systems is essential. The inventory should mention the site and purpose of the computerised system. This list should indicate the risk assessed category of each system. Systems that have an influence on regulated activities need to be identified."* Note that the GxP-relevance might change when the ***current range of functionality*** *of* the system is shifting.

As with GAMP 5[i] the role of the ***suppliers and service providers*** becomes more obvious and critical in the new annex 11. Suppliers of software and services are rated critical to GMP and consequently they need to be treated just like suppliers of APIs or excipients i.e. they should be assessed and may be subject to an audit. Where the current annex 11 only states one sentence the new annex 11 provides the requirements in four detailed sub parts (please refer to table 2 Suppliers and Service Providers below). Nota bene: ***IT-departments should be considered analogous*** to third parties and ***audit information relating to suppliers or developers of software and implemented systems should be made available to inspectors on request.*** The regulated user will need to establish a policy on how much details of such audit information he will report to the inspector.

The somehow vague term "key ***personnel***" in the current annex 11 is very precisely defined now *"There should be close cooperation between all relevant personnel such as* ***Process Owner, System Owner, Qualified Persons and IT.****"* The terms Process Owner and System Owner are explained in the ***Glossary*** (a new feature of this annex) and the explanation are nearly exact copies of the GAMP 5 definition [words in brackets are not transferred from GAMP 5]:

Process Owner

The person [ultimately] responsible for the business process [or processes being managed].

Based on this definition PharmAdvice recommends that the Process Owner should finally sign and release User Requirement Specifications.

System Owner

The Person [ultimately] responsible for the availability [, and support] and maintenance of a system and for the security of the data residing on that system.

This definition seems equally clear at first glance. However, who will be the **System Owner** may not be so easy to decide. One might get the impression that someone from IT may be appropriate as he or she will be the right SME (subject matter expert[ii]) for designing or releasing system design specifications, backup and archiving procedures, security measures etc. However as IT departments should be treated as "third parties" there is some conflict. Clearly, a third party can care about system availability etc, but it is PharmAdvice's opinion, that the third party will not be ultimately responsible. So the System Owner should rather be from business but needs to have a good understanding of IT.

The ***Project Phase*** section of annex 11 is completely dedicated to validation.

- Notwithstanding the possibility to leverage system life cycle documentation supplied by the supplier for the ***validation***, Annex 11-01-2011 stresses the responsibility of the regulated user demanding "*Manufacturers should be able to **justify** their **standards, protocols, acceptance criteria,** procedures and records based on their risk assessment."* This applies equally to ***commercial off-the-shelf products*** as well as ***bespoke or customised computerised systems.*** The requirement that ***"**Documentation supplied with commercial off-the-shelf products should be reviewed by regulated users to **check that user requirements are fulfilled**"*** implicates that URS should be formally available not only for GAMP category 4 and 5 but also for GAMP category 3 systems. By the way this request is in line with the 2001 US FDA draft Guidance for Industry, 21 CFR Part 11; Electronic Records; Electronic Signatures: Validation validation_cfr11. Though this guidance has been withdrawn in 2003 the sentence "*Without first establishing end user needs and intended uses, we believe it is virtually impossible to confirm that the system can consistently meet them"* is still logical and therefore remains valid. Of course this does not impy that the URS for GAMP category 3 systems need to be as detailed as specifications for bespoke systems; however the need to indicate which functionality is required and critical to GMP.
  Compared to the 2008 draft the level of detail concerning ***validation*** has been cut in half. Detailed requirements for validation of database based/inclusive systems and spreadsheets have been removed. However this does not mean that those requirements in the 2008 draft for spreadsheets need not be considered. In line with the 2008 draft PharmAdvice strongly recommends that "*Spreadsheets should be suitably checked for accuracy and reliability and stored in a manner which ensures the appropriate version control. The calculations should be secured in such a way that formulations are not intentionally or accidentally overwritten. … Formulations should also be protected from accidental input of in appropriate data type…".*
  Concerning testing the new annex 11 emphasizes the requirement to include negative testing demanding *"**Evidence of appropriate test methods** and test scenarios should be demonstrated. **Particularly, system (process) parameter limits, data limits and error handling** should be considered."*

The section on the ***Operational Phase*** is subdivided into 13 subsections. In short the annex 11 describes what in practice needs a lot of well organized procedures.

- Built-in checks for the correct entry and processing of data are explicitly required when ***data*** are exchanged electronically.

- As manual data entry is an important source of error, critical data entered manually need to be subjected to ***accuracy checks***. It is up to the regulated user to analyze ***potential consequences*** on ***erroneous or incorrectly entered data*** and define appropriate checks.

- ***Data Storage*** needs to be ***secure***, both physically and electronically. The **ability to restore back-ups accurately** needs to be **periodically monitored**; this implies not only that required hard- and software is available but also that the data can be correctly processed. Procedures need to be in place to define who is authorized to initiate a back-up of data and how any potential adverse effect to most recent data is assessed.

- Clear ***printouts*** of electronically stored data may be requested by the inspectors and for all records supporting batch release it should be possible to *generate printouts indicating if any of the data has been changed since the original entry*.

- A risk assessment is required to define which data need to be subject to an ***audit trail.*** The requirement that ***audit trails*** *need to be available and* ***convertible to a generally intelligible form*** implies that a mere triggering and recording of changes in a database may not be sufficient. The 2008 draft of the annex explained the idea behind the audit trail as *the aim is to know at any given time point what the information was* and clearly stated that changed data should be available in their appropriate context: *For example if a relevant electronic record is created using a number of data fields, all these data fields need to be linked within the audit trail.*

- Exactly as required for any other GMP-relevant process a ***Change and Configuration Management*** needs to be established to guarantee that ***changes to a computerised system*** *including system configurations should only be* ***made in a controlled manner in accordance with a defined procedure***.

- Also, following a general GMP-requirement ***periodic evaluation*** needs to demonstrate that the computerized system is still compliant to GMP. The EU GMP annex 11 explicitly requires the following items to be evaluated : ***current range of functionality, deviation records, incidents, problems, upgrade history, performance, reliability, security and validation status reports.***

- *Physical and/or logical controls should be in place to* ***restrict access to computerised systems***, therefore ***creation, change, and cancellation of access authorisations should be recorded.*** *Mechanisms for the detection of attempts of unauthorised access* as required in the 2008 draft annex are no longer explicitly demandedas part of ***Security.*** When document or data management systems are used these *should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.* There is no explicit requirement how this time stamp should be configured; PharmAdvice recommends considering using UTC instead of a local time zone especially in process equipment and continuous processes.

- ***Incident Management*** shall ***report and assess all incidents, not only system failures and data errors****, the root cause of a critical incident should be identified and should form the basis of corrective and preventive actions*. This requirement is considerably more challenging than the current requirement to *record and analyse errors and to enable corrective action to be taken.* However it is consonant with section 5.46 of Part II of the EU guide: Basic Requirements for Active Substances used as Starting Materials requesting *Incidents related to computerized systems that could affect the quality of intermediates or APIs or the reliability of records or test results should be recorded and investigated.*

- ***Electronic signatures*** *are expected to:*
  a. have the same impact as hand-written signatures within the boundaries of the company,
  b. be permanently linked to their respective record,
  c. include the time and date that they were applied.
  The restriction ***within the boundaries of the company****,*is very important, because it indicates that there is no requirement for a "qualified electronic signature".

- *When a computerised system is used for recording certification and* ***batch release*** only Qualified Persons may be allowed to release the batch placing their **electronic signature.** Obviously **it is the intention to avoid hybrid systems with handwritten signatures to records stored and maintained electronically.**

- Arrangements to provide ***business continuity*** to bring manual or alternative back-up computerized systems into use needs to be **adequately documented and tested,** if the computerised system supports a critical process. The restriction to *critical regulatory or lifesaving processes* mentioned in the 2008 draft has been removed. Again it is up to the regulated user to perform a risk assessment and define how fast the alternative system must be operative.

- Though storage capacities permanently increase considerably the annex 11 accepts that ***data may be archived,*** i.e. removed from immediate system access. Migration plans are required *if relevant changes are to be made to the system (e.g. computer equipment or programs)* and *the ability to retrieve the data should be ensured and tested.* This is a very challenging task in practice as different data need to be available for different required retention periods defined by predicate rules.

Table: Risk based Approach of EU Annex 11	Chapter
Current annex 11:	
*Consideration should be given to the **risk** of losing aspects of the previous system which could result from reducing the involvement of operators.*	Principles
Annex 11-01-2011:	
*There should be no increase in the overall **risk** of the process.*	Principles
***1 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**.*	General ***Risk Management***
*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**.*	General *Suppliers and Service Providers*
*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***	Project Phase: *Validation*
*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.*	Project Phase: *Validation*
5. Data *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.***	Operational Phase: *Data*
6. Accuracy Checks *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**.*	Operational Phase: *Accuracy Checks*
9. Audit Trails *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").*	Operational Phase: *Audit Trails*
16. Business Continuity *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.*	Operational Phase: *Business Continuity*
EUROPEAN COMMISSION HEALTH AND CONSUMERS DIRECTORATE-GENERAL Public Health and **Risk Assessment** **Pharmaceuticals**	Document Header

Table 2: Suppliers and Service Providers	Chapter
Current annex 11:	
When outside agencies are used to provide a computer service, there should be a formal agreement including a clear statement of the responsibilities of that outside agency (see Chapter 7).	System 18
Annex 11-01-2011:	
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****.*	*General* *3. Suppliers and Service Providers*
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.***	

Table 3: Comparison of Annex 11 versions

Current Annex 11		***Annex 11 Draft 2008***		***Annex 11-01-2011*** **(valid from 30 June 2011)**	
2 pages	**section**	**8 pages**	**section**	**4 pages**	**section**
Principle		Principle		***Principle***	
				General	
		Risk Management	1 (1.1)	Risk Management	1
Personnel	1	Personnel	2 (2.1)	Personnel	2
				Suppliers and Service Providers	3 (3.1 to 3.4)
				Project Phase	
ion	2	Validation	3 (3.1 to 3.8)	Validation	4 (4.1 to 4.8)
				Operational Phase	
System	3 - 19	System	4 (4.1 to 4.2)		
		Software	5 (5.1 to 5.3)		
		Data	6 (6.1)	Data	5
		User Testing and system's fitness for purpose	7 (7.1)		
		Security	8 (8.1 to 8.5)	Security	12
		Accuracy Checks	9 (9.1 to 9.2)	Accuracy Checks	6
		Audit Trails	10 (10.1)	Audit Trails	9
		Signatures	11 (11.1)	Electronic Signature	14
		Change control and configuration management	12 (12.1)	Change and configuration management	10
		Printouts	13 (13.1)	Printouts	8 (8.1 to 8.2)
		Data Storage	14 (14.1)	Data Storage	7 (7.1 to 7.2)
		Back Up; Migration; Archiving; Retrieval	15 (15.1 to 15.3)	Archiving	17
		Busisness Continuity	16 (16.1)	Busisness Continuity	16
		Incident Management	17 (17.1)	Incident Management	13
		Suppliers	18 (18.1 - 18.2)		
		Batch Release	19 (19.1)	Batch Release	15
				Periodic Review	11
				Glossary *Application, Bespoke/ Customised computerised system, Commercial of the shelf software, IT Infrastructure,Life cycle, Process Owner, System Owner, Third Party*	

compiled by Dr. Manfred Müller www.pharmadvice.de

The table below represents the question part of the Excel file, please ask for the complete file with answers, automatic score and evaluation.
mailto:manfred.mueller@pharmadvice.de
By the way, for those interested in Excel, the File will demonstrate multi stage conditional formatting and validity check on data input and many other features which can advantageously be used to render an Excel file GMP-compliant.

Playfully test your knowledge on the new EU annexx 11 on computerised systems				www.pharmadvice.de
macros need to be enabled				**0 answers given / 34 remaining**
delete all answers / show Manfred's answers / Hide Manfred's answers / view instructions / view disclaimer				
		correct	not correct	
1	According to annexx 11 published January 2011 "Risk management should be applied **throughout the lifecycle** of the computerized system."			
2	The idea of a risk based validation is completely new to annexx 11			
3	"Where a computerised system replaces a manual operation, there should be no resultant decrease in product quality, process control or quality assurance." is the basic principle of annexx 11			

4	Name the 4 groups of persons which are explicitely required to cooperate when computerised systems are used within GMP areas.			
5	It is advantegeous to use the companies IT-department to provide and validate a computerized system because they will operate according to the pharmaceutical companies standards and **therefore there is no need for formal agreements.**			
6	As the competence and reliability of a supplier are key factors when selecting a product or service provider every supplier needs to be audited. Quality system and audit information relating to suppliers or developers of software should be made available to (authorities) inspectors on request.			
7	An **up to date listing** of all computerized systems used in GMP areas needs to be maintained by the pharmaceutical company.			
8	Critical data entered manually need to be verified by a second person.			
9	Evidence of appropriate test methods and test scenarios should be demonstrated. Name the 3 items which should be considered in particular.			

10	User Requirements Specifications should describe the required functions of the computerised system and be based on documented risk assessment and GMP impact. User Requirements are required during the project phase and for customized systems or bespoke systems only.			
11	Data should be secured by both physical and electronic means against damage. Name the 3 items which need to be checked throughout the retention period.			
12	Regular back-ups of all relevant data should be done. Name the 3 items which need to be monitored periodically.			
13	When database applications are used within a regulated environment a listing of the database tables and the changes to the data within these tables is generally sufficient to provide an appropriate audit trail.			
14	Any change to a computerised system including system configurations requires re-validation.			

15	Periodic evaluation Computerised systems should be periodically evaluated to confirm that they remain in a valid state and are compliant with GMP. Please name all items which need to be evaluated.			
16	When a computerised system is used for recording certification and batch release, a cryptographically based digital signature must be used to clearly identify and record the person releasing or certifying the batches.			
17	When using this Excelfile to proof employees have read and understood the new EU annexx 11 validation of this file is NOT required because Microsoft Excel is a well established commercial of the shelf software.			

Please enable to show the answers and my score as soon as I have given at least the following number of answers	21	
Set your target for the evaluation		
good >	80	%
I can do better >	50	%
improvement needed <=	50	%

Example of answer evaluation, demonstrating conditional formatting

			28 correct answers = 82,4 % of all possible correct answers
	correct	not correct	
correct answer	x		
you need to decide, you can't select both answers	x	x	
wrong answer		x	
text question, correct answer selected			Process Owner
no duplicates please			System Owner
wrong answer			CEO
			System Owner

[i] GAMP 5 A Risk-Based Approach to Compliant GxP Computerized Systems, ISPE 2008, Appendix S3

[ii] according to GAMP 5 "*Those individuals with specific expertise in a particular area or field.")*