propharma

VALIDATION CENTER

Annex 11 Introduction

v.25.03

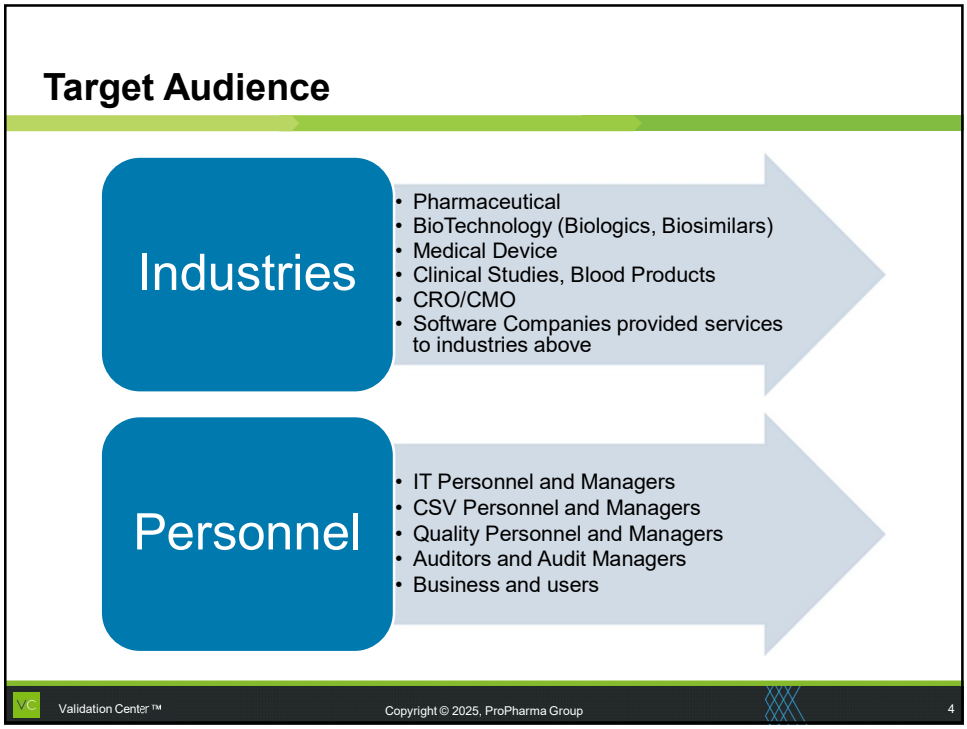
1

Your Presenter

- Esra Guven, BScEE, PMP, ASQ SSGB
- Associate Director, Computer Systems Validation and Data Integrity ProPharma Group
- 25+ years of experience in IT Quality and Computer Systems Validation within the Pharmaceutical Industry.
- Expert on:
  - Computer Systems Validation (CSV)
  - Computer Software Assurance (CSA)
  - Data Integrity (DI)
  - IT Quality and Compliance
  - Electronic Records and Signatures
  - Agile / Lean CSV

2

3



4

Annex 11 Webinar Outline

1. EU Terminology
2. Annex 11 History & Applicability
3. Inside Annex 11
4. Future of Annex 11
5. Annex 11 vs. Part 11
6. Related Regulations & Guidelines

Validation Center™ Copyright © 2025, ProPharma Group 5

5

EU Terminology

Part 1

Validation Center™ Copyright © 2025, ProPharma Group 6

6

Part 1: EU Terminology

- Section Overview
  - EU Organizations and Roles
  - Structure of EU Regulations for Medicinal Products

7

EU (European Union)

- 27 Member States
- Single market
- Standardized laws
- ~450 million people
- ~20% of global GDP

Austria	Italy
Belgium	Latvia
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czech Republic	Netherlands
Denmark	Poland
Estonia	Portugal
Finland	Romania
France	Slovakia
Germany	Slovenia
Greece	Spain
Hungary	Sweden
Ireland	

8

EC (European Commission)

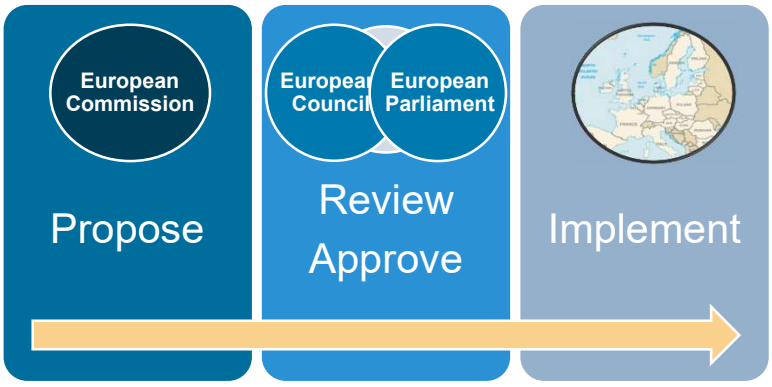
Commission Responsibilities

- Proposing legislation
- Implementing decisions
- Upholding EU treaties
- Managing EU business

9

Directives

- **Directives:** Legal acts that require EU member states to achieve a specified result



10

EudraLex

- **EudraLex:** Rules (legislation) governing medicinal products within the European Union

Volume 1 EU pharmaceutical legislation for medicinal products for human use	Volume 2 Notice to applicants and regulatory guidelines for medicinal products for human use	**Volume 3** Scientific guidelines for medicinal products for human use	**Volume 4** Guidelines for good manufacturing practices for medicinal products for human and veterinary use	**Volume 5** EU pharmaceutical legislation for medicinal products for veterinary use
Volume 6 Notice to applicants and regulatory guidelines for medicinal products for veterinary use	**Volume 7** Scientific guidelines for medicinal products for veterinary use	**Volume 8** Maximum residue limits	**Volume 9** Guidelines for pharmacovigilance for medicinal products for human and veterinary use	**Volume 10** Guidelines for clinical trials

11

EudraLex Volume 4

Volume 4
Guidelines for good manufacturing practices for medicinal products for human and veterinary use

Part 1: Basic Requirements for Medicinal Products

Chapter 1 Pharmaceutical Quality System	**Chapter 2** Personnel	**Chapter 3** Premise and Equipment
Chapter 4 Documentation	**Chapter 5** Production	**Chapter 6** Quality Control
Chapter 7 Outsourced Activities	**Chapter 8** Complaints and Product Recalls	**Chapter 9** Self Inspection

Part 2: Basic Requirements for Active Substances Used as Starting Materials — Basic Requirements

Part 3: GMP-Related Documents

Site Master File | MRA Batch Notif-ication | Q9 Quality Risk Manage-ment | Q10 Pharma-ceutical Quality System | Templates & Guides

Annexes

Annex 1 Sterile Products	Annex 10 Aerosol Preparations
Annex 2 Biological Substances	Annex 11 Computerised Systems
Annex 3 Radiopharmaceuticals	Annex 12 Ionising Radiation
Annex 4 Veterinary Products 1	Annex 13 Investigational Prods.
Annex 5 Veterinary Products 2	Annex 14 Blood/Plasma Prods.
Annex 6 Medicinal Gases	Annex 15 Qualification/Validation
Annex 7 Herbal Products	Annex 16 QP Cert/Batch Release
Annex 8 Material Sampling	Annex 17 Parametric Release
Annex 9 Liquids, Creams, …	Annex 19 Reference Samples

12

EMA (European Medicines Agency)

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Agency Responsibilities

- Coordinate evaluation and monitoring of centrally authorized EU products
- Develop technical guidance
- Provide scientific advice

13

Annex 11 History & Applicability

Part 2

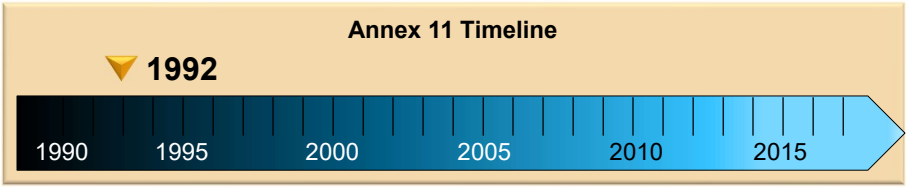
14

Part 2: Annex 11 History & Applicability

- Section Overview
  - Annex 11 History: Development, Revision, and Implementation
  - Annex Applicability: Countries, Products, Processes, Systems

15

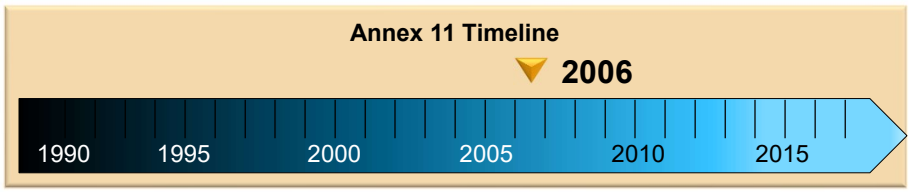
Introduction



- Annex on “Computerised Systems” was added to 2nd version of EudraLex GMP Guidelines

16

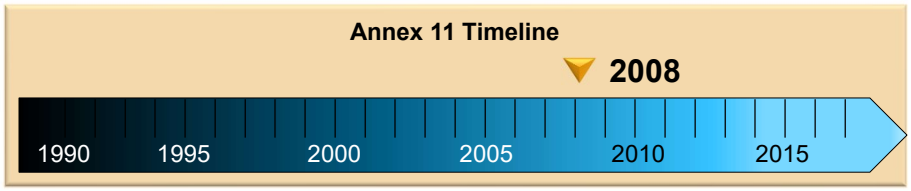
Revisions Initiated



- EMEA recommended a committee to update
  - Annex 11 Computerised Systems
  - Chapter 4 Documentation

17

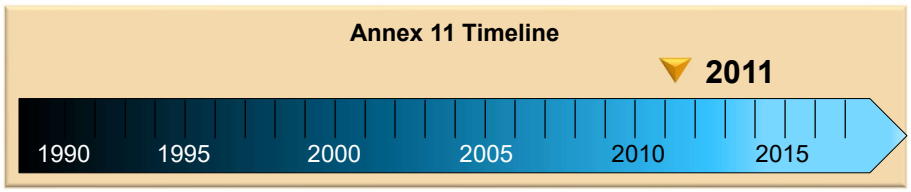
Draft Prepared and Reviewed



- Working Group released drafts for public comment
  - Annex 11 Computerised Systems
  - Chapter 4 Documentation
- Feedback collected for 6 months

18

Final Version



- Final versions published
  - Annex 11 Computerised Systems
  - Chapter 4 Documentation
- New versions in effect

19

To Which Companies Does Annex 11 Apply?

Companies that **manufacture***

*
- Purchase/receipt of materials
- Production
- Filling
- Labelling
- Quality Control
- Release
- Storage
- Distribution

medicinal products** for human or veterinary use

**
- Pharmaceuticals
- Radio-pharmaceuticals
- Biological products
- Blood/Plasma based products
- Vaccines
- Homeopathic medicinal products
- Herbal medicinal products
- Advanced therapies

within and/or for the **European Union**

- Annex 11 applies to companies manufacturing within the EU
- Companies outside the EU must conform to equivalent standards when manufacturing products for export to the EU

20

Systems… *examples*

Software used in the production of the product

- Manufacturing Automation Software
- Material Control Software
- Laboratory Instrument Software
- Batch Release Software
- Programmable Logic Controllers (PLCs)
- Building Management Systems
- Laboratory Management Software
- Labeling Software

Software used to implement the quality management system

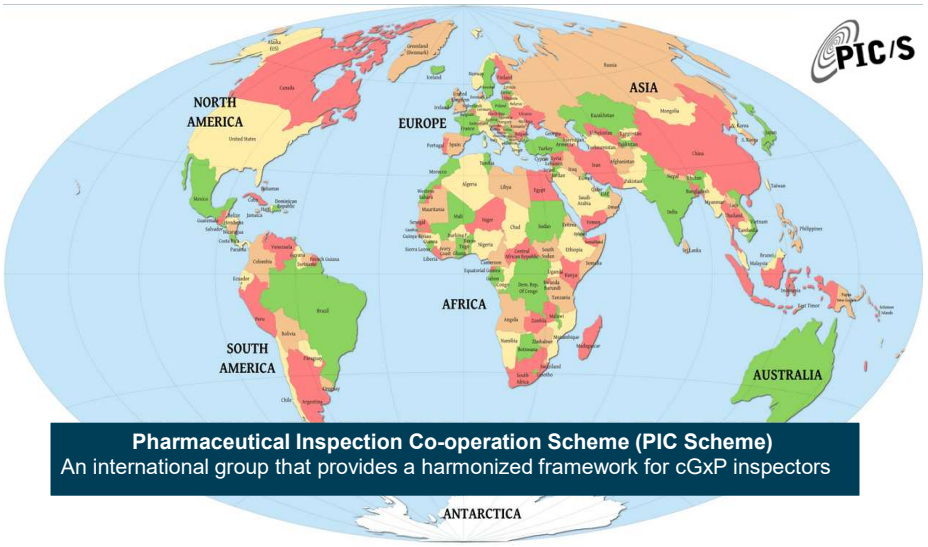
- Inventory Control Software (e.g., ERPs)
- Calibration Software
- Document Management Software
- Deviation Tracking Software
- Product Returns Management Software
- Quality Trending Software
- Complaints Software
- CAPA Software

Other software used to create or retain records

- Warehouse Management Software
- Supplier Approval Records
- Training Records Software
- Distribution Records

21

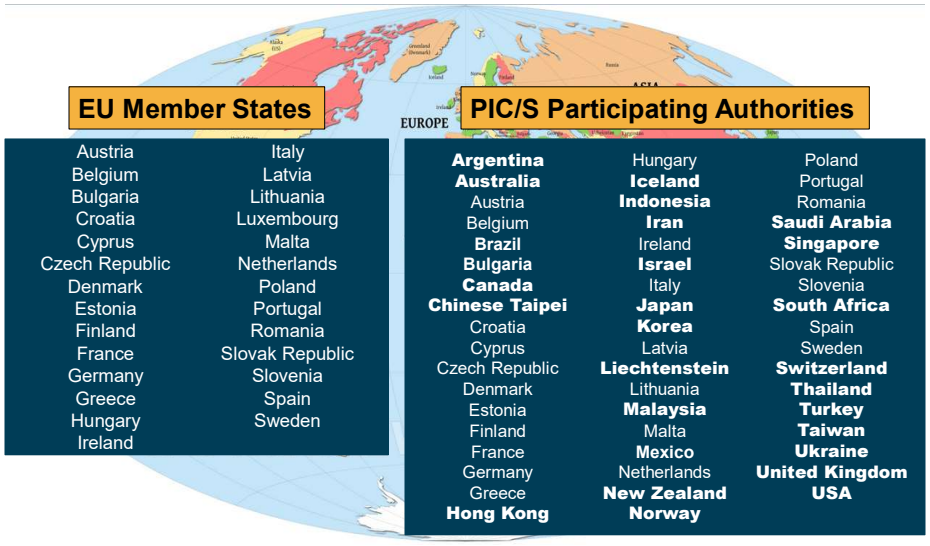
PIC/S



Pharmaceutical Inspection Co-operation Scheme (PIC Scheme)
An international group that provides a harmonized framework for cGxP inspectors

22

Annex 11 Applicable Countries



EU Member States

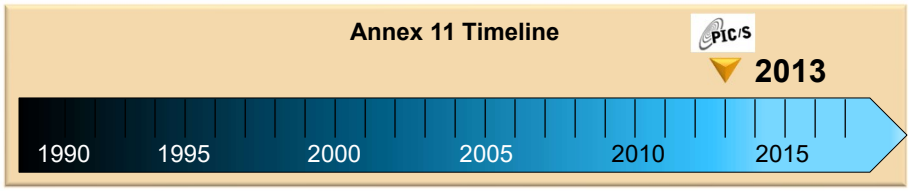
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
Poland
Portugal
Romania
Slovak Republic
Slovenia
Spain
Sweden

PIC/S Participating Authorities

Argentina
Australia
Austria
Belgium
Brazil
Bulgaria
Canada
Chinese Taipei
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hong Kong
Hungary
Iceland
Indonesia
Iran
Ireland
Israel
Italy
Japan
Korea
Latvia
Liechtenstein
Lithuania
Malaysia
Malta
Mexico
Netherlands
New Zealand
Norway
Poland
Portugal
Romania
Saudi Arabia
Singapore
Slovak Republic
Slovenia
South Africa
Spain
Sweden
Switzerland
Thailand
Turkey
Taiwan
Ukraine
United Kingdom
USA

23

PIC/S Adoption



- Incorporated into PIC/S GMPs
  - Annex 11 Computerised Systems
  - Chapter 4 Documentation

24

PIC/S GMP Guide

PE 009
Guide to Good Manufacturing Practice for Medicinal Products

Part 1: Basic Requirements for Medicinal Products

Quality Management	Personnel	Premises and Equipment
Documentation	Production	Quality Control
Contract Manufacture	Complaints and Product Recall	Self Inspection

Part 2: Basic Requirements for Active Ingredients

Quality Management	Personnel	Buildings & Facilities
Process Equipment	Documentation & Records	Materials Management
Production Controls	Packaging and Labeling	Storage and Distribution
Laboratory Controls	Validation	Change Control
Rejection and Re-use	Complaints and Recalls	Contract Manufacturing
Distributors, Re-labellers	Cell Culture/ Fermentation	APIs for Clinical Trials

Annexes

Annex 1 Sterile Products	Annex 10 Aerosol Preparations
Annex 2 Biological Substances	Annex 11 Computerised Systems
Annex 3 Radiopharmaceuticals	Annex 12 Ionising Radiation
Annex 4 Veterinary Products 1	Annex 13 Investigational Prods.
Annex 5 Veterinary Products 2	Annex 14 Blood/Plasma Prods.
Annex 6 Medicinal Gases	Annex 15 Qualification/Validation
Annex 7 Herbal Products	Annex 16 QP Cert/Batch Release
Annex 8 Material Sampling	Annex 17 Parametric Release
Annex 9 Liquids, Creams, …	Annex 19 Reference Samples
Annex 20 Quality Risk Mgmt.	

25

Inside Annex 11

Part 3

26

Part 3: Inside Annex 11

- Section Overview
  - Definitions
  - Expectations
  - Actions for Compliance

27

Definitions

Computerised System

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

Application
Software installed on a defined platform/hardware providing specific functionality

IT Infrastructure
The hardware and software such as networking software and operation systems, which makes it possible for the application to function

Bespoke/Customised

A computerised system individually designed to suit a specific business process

Commercial off the Shelf
Software commercially available, whose fitness for use is demonstrated by a broad spectrum of users

aka. COTS

28

Definitions

Process Owner

The person responsible for the **business process**

Third Party

Parties **not directly managed** by the holder of the manufacturing and/or import authorisation

System Owner

The person responsible for the **availability**, and **maintenance** of a computerised system and for the **security** of the data residing on that system

29

Personnel [Annex 11 Section 2]

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

Actions for Compliance	Establish the qualifications for each role	Document each person's qualifications for their role	Establish the qualifications for each system access level	Document each person's qualifications for their access level

30

Risk Management [Annex 11 Section 1]

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

Actions for Compliance

Establish a standard risk assessment procedure	Document a Risk Assessment for each system	Establish the validation and other quality requirements for each risk level	Utilize requirements in making decision for each system

31

Validation [Annex 11 Section 4]

- An **up-to-date listing** of all relevant systems and their GMP functionality (inventory) should be available.

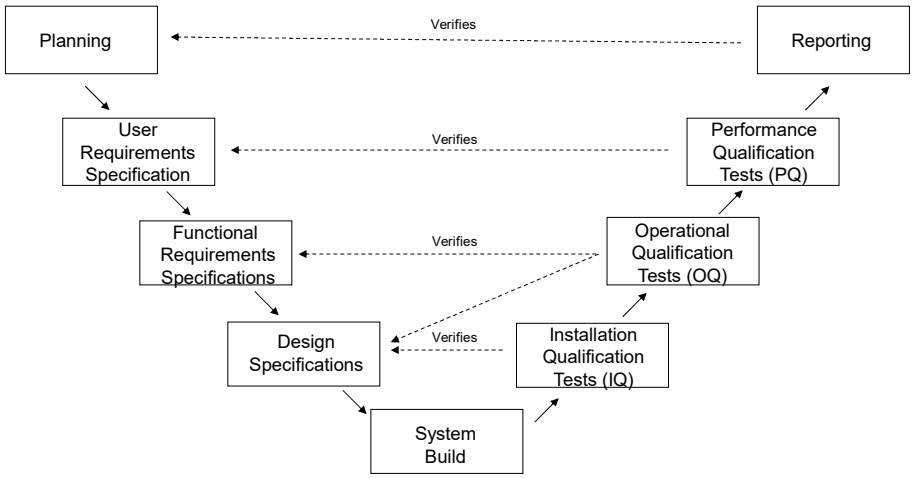
Actions for Compliance

Create an inventory of systems.
Establish procedure to keep inventory up-to-date

System/ Software Name	Version	GxP Functionality	Risk Level	Validation Status	Last Validation Date	Next Validation Date	Next Periodic Review Date

32

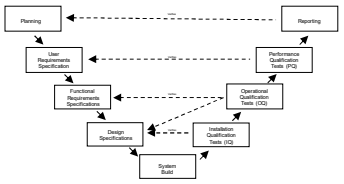
Validation Process



33

Validation [Annex 11 Section 4]

- The validation documentation and reports should **cover the relevant steps** of the life cycle.



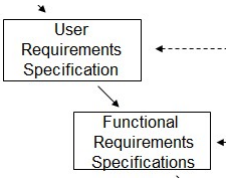
- Should be able to justify standards, protocols, acceptance criteria, procedures and records **based on their risk assessment**.

Actions for Compliance				
	Establish validation requirements for each risk level	**Document a Risk Assessment for each system**	**Utilize requirements in making decision for each system**	**Document the validation decisions for the system, e.g. Validation Plan**

34

Validation [Annex 11 Section 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.



Actions for Compliance				
	Document the User Requirements for each system	Ensure requirements appropriate for risk-level and GMP compliance	Trace user requirements to risk levels and to functional requirements	Trace user requirements to validation testing

35

Validation [Annex 11 Section 4]

- 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.

Actions for Compliance			
	Document a Risk Assessment for each system	Document the Design, especially for Critical systems	Update Design when changes are made to the system

36

Validation [Annex 11 Section 4]

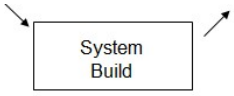
- The **regulated user** should take all reasonable steps to ensure that the system has been developed in accordance with an **appropriate quality management system**.
- The supplier should be **assessed** appropriately.
- Documentation supplied with Commercial-off-the-Shelf products should be **reviewed by regulated users to check that user requirements** are fulfilled.

Actions for Compliance				
	Document a Risk Assessment for each system	Establish vendor assessment approach for each risk level	Assess vendor's quality management practices and documentation	Define validation activities and approach based on assessment

37

Validation [Annex 11 Section 4]

- 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.

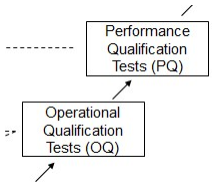


Actions for Compliance			
	Establish standard development and validation procedures	Assess the quality and performance of custom-built systems during build	Continue to assess quality and performance after deployment

38

Validation [Annex 11 Section 4]

- Evidence of appropriate **test methods and test scenarios** should be demonstrated. Particularly, system parameter limits, data limits and error handling should be considered.
- Automated testing **tools** and test **environments** should have documented assessments for their adequacy.



Actions for Compliance				
	Establish testing requirements for each risk level	Apply these testing requirements to each system or feature	Document risk level for testing tools. Demonstrate adequacy (risk-based)	Demonstrate adequacy of validation testing environment, e.g., via IQ

39

Validation [Annex 11 Section 4]

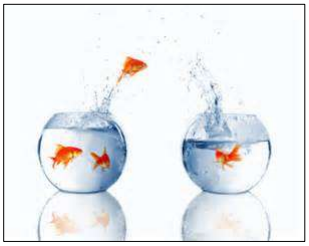
- Validation documentation should include **change control** records (if applicable) and reports on any deviations observed **during** the **validation** process.

Actions for Compliance				
	Establish procedure for Change Management during validation	Document any changes made during validation	Assess impact of all changes to identify re-testing needed	Document any exceptions (deviations)

40

Validation [Annex 11 Section 4]

- 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.



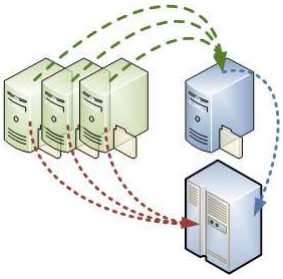
Actions for Compliance

- **Validate data transfers between systems**
- **Include testing to verify that data is not altered**

41

Data [Annex 11 Section 5]

- 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.



Actions for Compliance

- **Design data exchanges for security and accuracy**
- **Validate data exchanges**

42

Data Accuracy [Annex 11 Section 6]

- 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.

Actions for Compliance				
	Refer to system Risk Assessment to identify data risk levels	Design functionality to reduce data entry errors	Validate functionality intended to reduce data entry errors	Establish procedures to catch any additional data entry errors

43

Audit Trails [Annex 11 Section 9]

- 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.

Actions for Compliance				
	Establish risk-based audit trail requirements	Ensure that systems meeting the risk threshold have audit trails	Verify that audit trails capture revisions, deletions and reasons	Validate the audit trail functionality

44

Audit Trails [Annex 11 Section 9]

- Audit trails need to be available and convertible to a generally **intelligible form** and **regularly reviewed**.

Actions for Compliance

Verify that audit trails can easily be reviewed

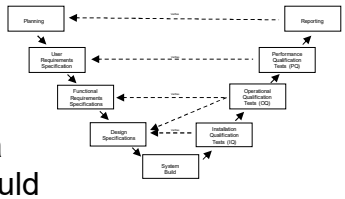
Establish risk-based procedures for reviewing audit trails

- How to review
- Who reviews
- What to look for
- How often to review
- How to document reviews

45

Data Storage [Annex 11 Section 7]

- Stored data should be checked for **accessibility, readability and accuracy**.
- Integrity and accuracy of backup data and the ability to restore the data should be checked **during validation and monitored periodically**.



Actions for Compliance

Validate the backup and restore functionality

Establish procedures to periodically check backups

- How to check
- Who checks
- How often to check
- How to document checks

46

Data Storage [Annex 11 Section 7]

- Data should be secured by **both physical and electronic** means against damage.
- Regular **back-ups** of all relevant data should be done.
- Access to data should be ensured **throughout the retention period**.

Actions for Compliance	**Design/Buy system to secure from internal & external threats**	**Secure and protect system from physical threats and damage**	**Implement back-up procedures**	**Retain data for retention period designated in regulations**

47

Data Archival [Annex 11 Section 17]

- 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.

Actions for Compliance	**Establish process to retrieve archived data**	**Test to verify that archived data can be retrieved and is accurate**	**If system is changed, update process to retrieve archived data**	**Test to verify that archived data can still be retrieved and is still accurate**

48

Security [Annex 11 Section 12]

- Physical and/or logical controls should **restrict access** to computerised system to authorised persons.
- Suitable methods of preventing unauthorised entry may include keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.
- The extent of security controls depends on the **criticality** of the computerised system.

Actions for Compliance		
	Design/Buy system to secure from internal & external threats	Secure and protect system from physical threats and damage

49

Security [Annex 11 Section 12]

- Management systems for data and for documents should be designed to record the **identity of operators**.
- Creation, change, and cancellation of access **authorisations should be recorded**.

Actions for Compliance				
	Design/Buy system to identify users	Validate user identification functionality	Establish procedures to record authorization of user access	Retain records of user access authorization, change, deletion

50

Electronic Signatures [Annex 11 Section 14]

- Electronic records may be signed electronically.
- 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.

Actions for Compliance	Design/Buy systems that meet e-sig requirements	Validate electronic signature functionality

51

Print Outs [Annex 11 Section 14]

- It should be possible to obtain **clear printed copies** of electronically stored data.
- For records *supporting batch release*, printouts should **indicate** if any of the data has been **changed** since the original entry.

Actions for Compliance	Design/Buy systems that meet the print out requirements	Validate print-out functionality

52

Batch Release [Annex 11 Section 14]

- When a computerised system is used for recording certification and batch release,
  - the system should allow **only Authorised 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**.

Actions for Compliance

- **Design/Buy systems that meet the batch release requirements**
- **Validate batch release functionality**

53

Incident Management [Annex 11 Section 13]

- 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.

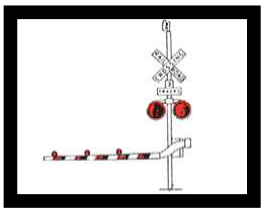
Actions for Compliance

- **Establish procedure for recording incidents**
  - Recording
  - Prioritizing
  - Investigating
  - Resolving
  - Escalating
  - Records
- **Establish procedure for incident investigation, correction, prevention**
  - Investigation
  - Correction
  - Prevention
  - Effectiveness
  - Tracking
  - Records

54

Change Management [Annex 11 Section 10]

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



Actions for Compliance

Establish process to control changes to system

- Change request documentation
- Impact assessment
- Change authorization
- Notifications
- Change record retention

55

Business Continuity [Annex 11 Section 16]

- 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).

Actions for Compliance

Use Risk Assessments to identify Critical processes

For each critical process, define an alternate plan

56

Business Continuity [Annex 11 Section 16]

- 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**.

Actions for Compliance				
	Use Risk Assessments to identify Critical processes	For each critical process, define an alternate plan	Document each alternate plan	Test the alternate plans

57

Periodic Evaluation [Annex 11 Section 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.

Actions for Compliance				
	Establish procedure for conducting Period Evaluations	Define and document risk-based schedule for Periodic Evaluation	Conduct Periodic Evaluations, per schedule	Document Evaluation outcomes and any corrections required

58

Periodic Evaluation [Annex 11 Section 11]

Actions for Compliance

Period Evaluations

What to Review…	Why to Review…
Current Regulations vs. system functionality	• Identify any gaps in system functionality (e.g., new e-sig regulations, new GMP regulations)
Current Use of System vs. User Requirements	• Identify features that were not originally validated • Identify features where risk level has changed
Validation Documents vs. Current Validation SOPs	• Confirm that old validation documents meet current validation requirements • Identify any missing documents
Change Requests	• Identify any gaps in validation testing • Identify out-of-date specification or design documentation • Identify out-of-date user SOPs and training materials
Incident Reports	• Identify new technical issues (security, performance, reliability, etc.) • Identify training gaps

59

Suppliers & Service Provider [Annex 11 Section 3]

Third Party

Parties
not directly managed
by the holder
of the manufacturing
and/or import authorisation

Suppliers and Service Providers include third parties that…

provide, install, configure, integrate, validate, maintain (e.g., via remote access), modify or retain a computerised system or related service or for data processing

60

Suppliers & Service Provider [Annex 11 Section 3]

- When third parties (e.g., suppliers, service providers) are used, **formal agreements** must exist between the parties, and these agreements should include clear statements of the responsibilities of the third party.
- IT-departments should be considered analogous.

Actions for Compliance			
	Establish minimum requirements for system vendor contracts	Review existing agreements vs. minimum requirements	Close gaps (i.e., implement, update agreements)

61

Suppliers & Service Provider [Annex 11 Section 3]

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

Actions for Compliance			
	Document a Risk Assessment for each system	Establish vendor assessment approach for each risk level	Assess vendor's quality management practices

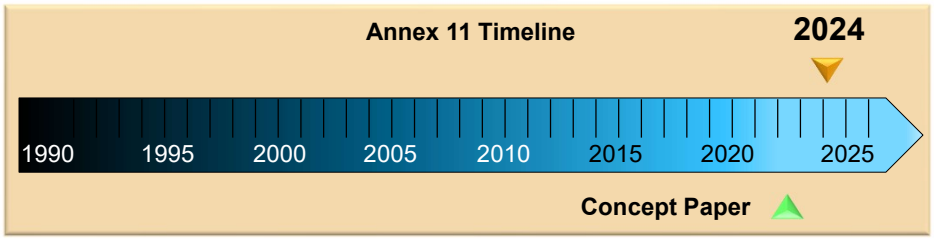
62

Future of Annex 11

Part 4

63

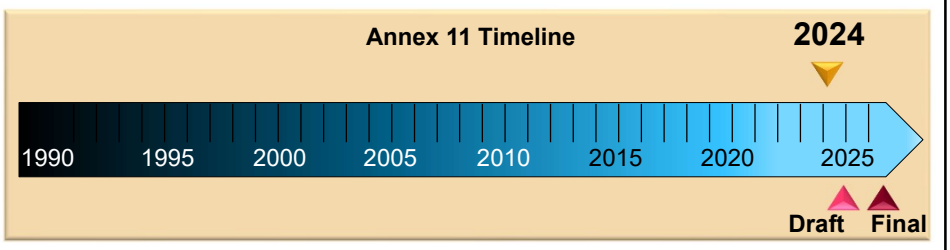
Annex 11 in the Future



- Announcement
  - **September 2022**: Intent to update Annex 11 announced via a Concept Paper

64

Annex 11 in the Future



- Timeline
  - **July 2025**: Publish draft updates for comment
  - **Oct 2025:** End feedback period on draft
  - **Oct 2026:** Adoption of updates to Annex 11 by EMA [EU]
  - **End 2026:** Publication of updated Annex 11

65

Drivers for Annex 11 Updates

Cloud Technology

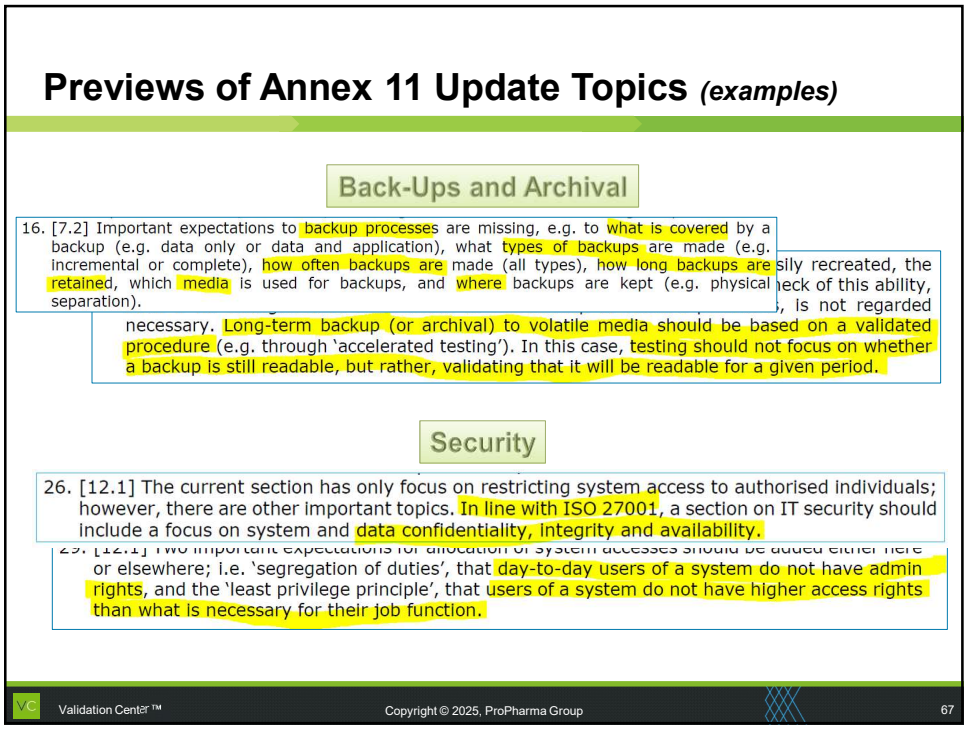
Agile Development Methodologies

New Security Technologies

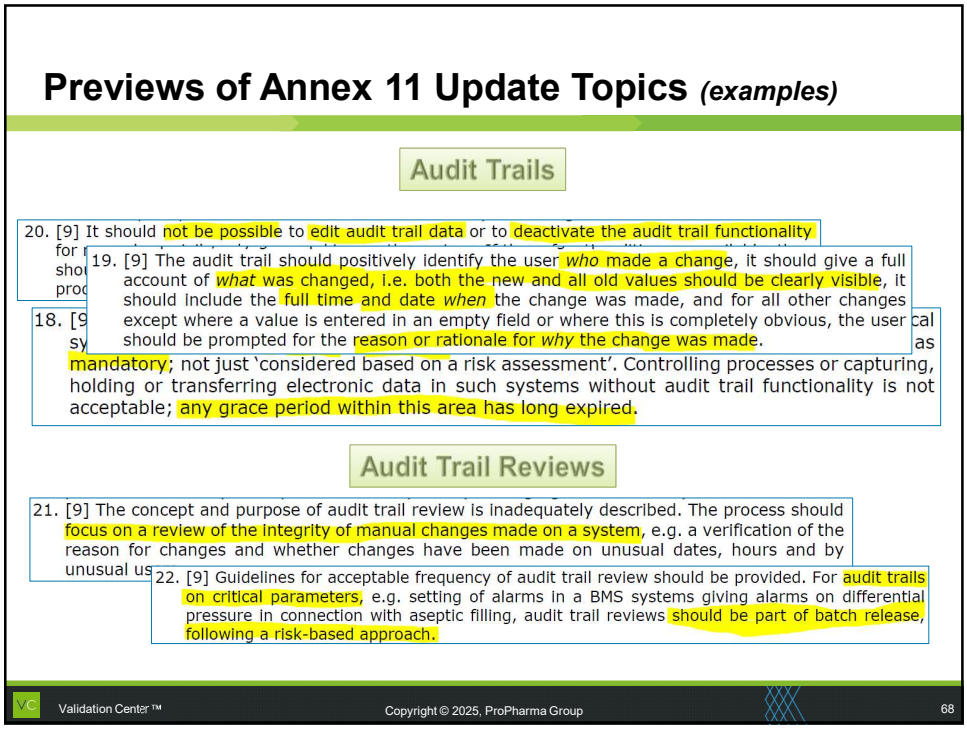
AI (artificial intelligence) and ML (machine learning)

Data Integrity Practices

66



67



68

Previews of Annex 11 Update Topics *(examples)*

Artificial Intelligence and Machine Learning

32. [New] There is an urgent need for regulatory guidance and expectations to the use of artificial intelligence (AI) and machine learning (ML) models in critical GMP applications as industry is already implementing this technology. The primary focus should be on the relevance, adequacy and integrity of the data used to test these models with, and on the results (metrics) from such testing, rather that on the process of selecting, training and optimising the models.

Access to Validation Documents

7. [3.1] For critical systems validated and/or operated by service providers (e.g. 'cloud' services), expectations should go beyond that "formal agreements must exist". Regulated users should have access to the complete documentation for validation and safe operation of a system and be able to present this during regulatory inspections, e.g. with the help of the service provider.

Computer Software Assurance (?)

33. [New] After this concept paper has been drafted and prepared for approval of the EMA GMP/GDP Inspectors Working Group and the PIC/S Sub-committee on GMDP Harmonisation, the FDA has released a draft guidance on Computer Software Assurance for Production and Quality System Software (CSA). This guidance and any implication will be considered with regards to aspects of potential regulatory relevance for GMP Annex 11.

69

Annex 11 vs. Part 11

Part 5

70

Part 5: Annex 11 vs. Part 11

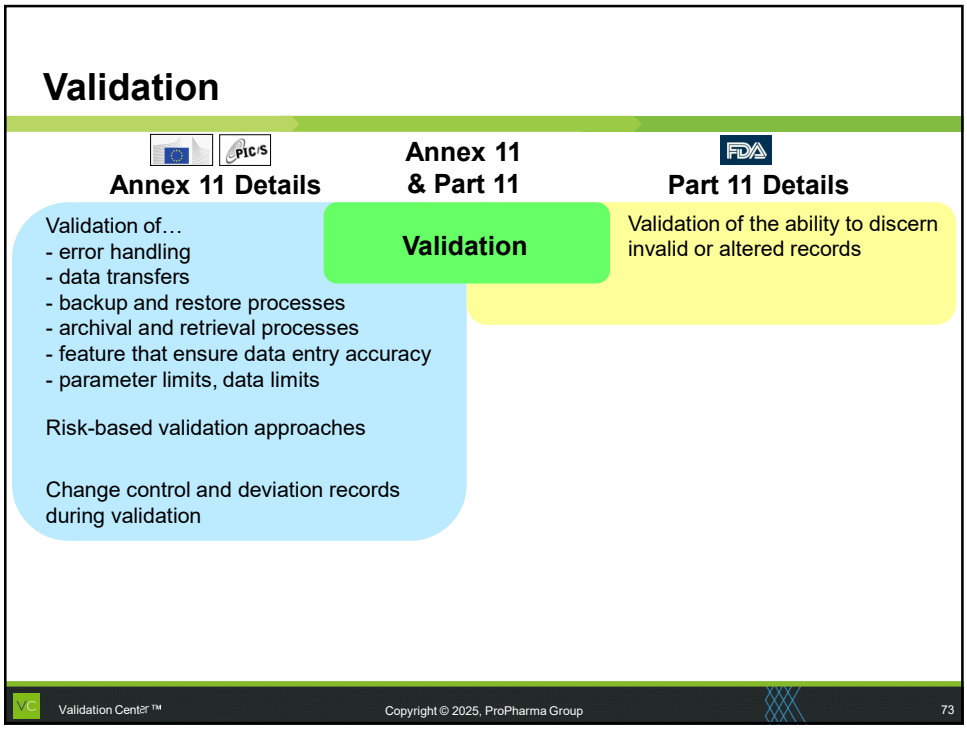
- Section Overview
  - System features
  - Validation
  - Documentation
  - Quality assurance processes

71

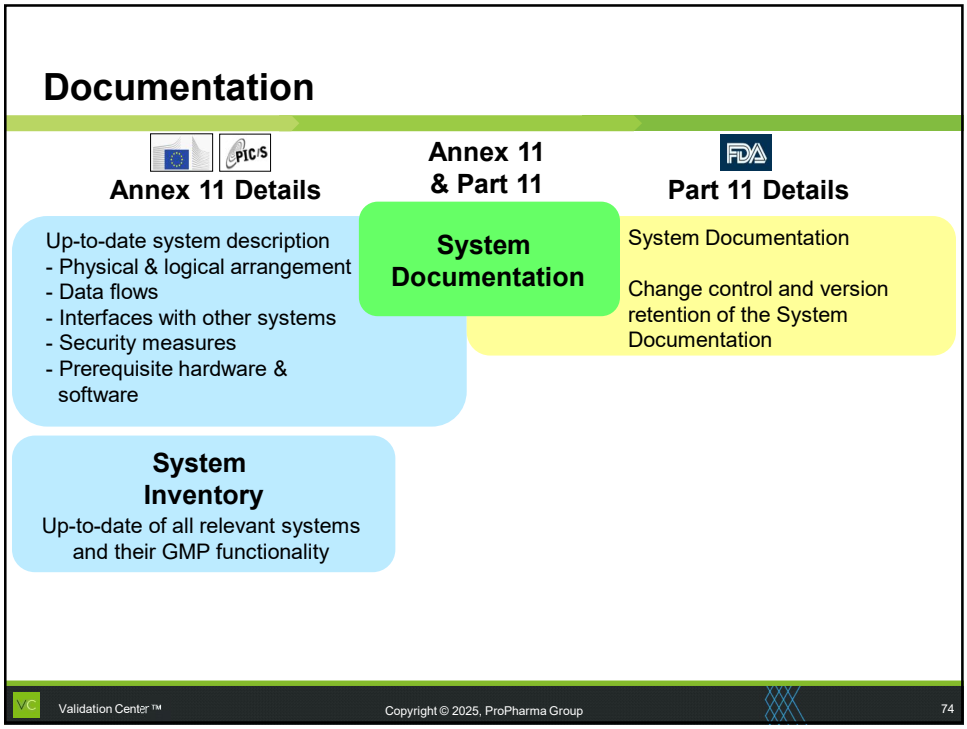
System Features and Functionality

Annex 11 Details	Annex 11 & Part 11	Part 11 Details
Accuracy checks for data exchanged with other systems and for manually entered data	**Accuracy, Integrity**	
Physical security	**Access Controls**	Periodic password revision Reporting unauthorized access attempts Device checks
Reason for change in audit trail	**Audit Trails**	Computer generated, automatic
Back-ups	**Retention, Protection**	Retention of audit trail records
Batch Release print-outs with change indicators	**Copies, Print Outs**	Audit trail available for review
E-Sig for batch release	**E-Signature**	E-Sig with printed name, meaning
		Confidentiality Open system confidentiality
		Sequencing Sequencing of system events

72



73



74

Quality Assurance Processes

Annex 11 Details	Annex 11 & Part 11	Part 11 Details
Periodic Review	Personnel Qualification	Lost/Stolen Passwords and Tokens
Audit Trail Review		Identity Verification
Back-Up Monitoring		
Access Authorization Records		
Incident & Investigation Records		
Critical Incident CAPA		
Change/Configuration Management		
Business Continuity Plans		
Supplier Management		
Risk Assessment & Management		
Manual Data Entry Review		

75

Related Regulations & Guidelines

Part 6

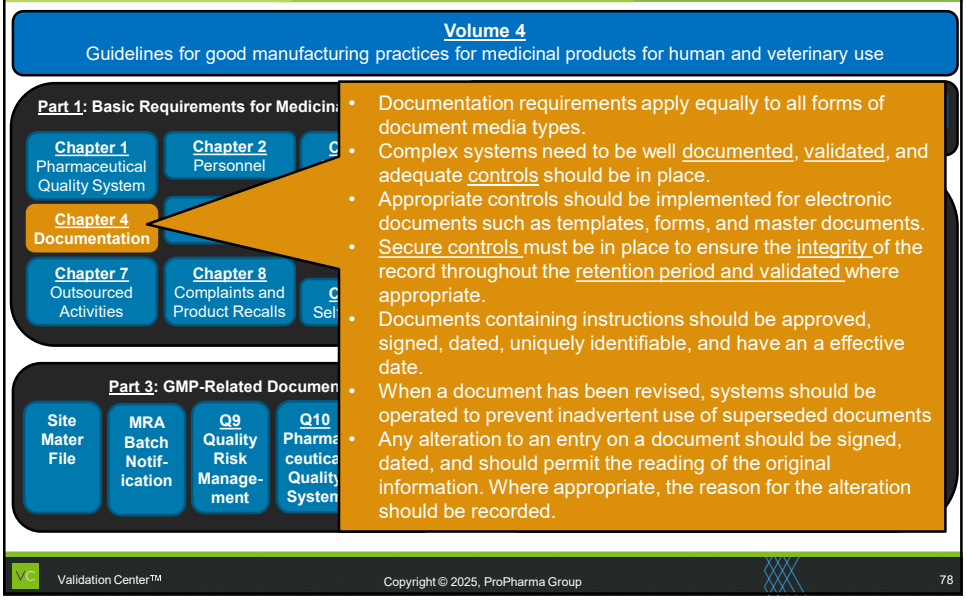
76

Part 6: Related Regulation & Guidelines

- Section Overview
  - Eudralex GMP Chapter 4
  - EMA Reflection Papers
  - PIC/S PI-011

77

EudraLex Volume 4, Chapter 4



78

EMA Reflection Papers

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Reflection Paper on Risk Based Quality Management in Clinical Trials

November, 2013

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Reflection Paper for Laboratories that Perform the Analysis or Evaluation of Clinical Trial Samples

February 2012

EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

Reflection Paper on Expectations for Electronic Source Data and Data Transcribed to Electronic Data Collection Tools in Clinical Trials

June 2010

79

PIC/S Good Practices for GxP Systems

PI 011
Good Practices for Computerised Systems Used in Regulated "GXP" Environments

Application Scope = GxP

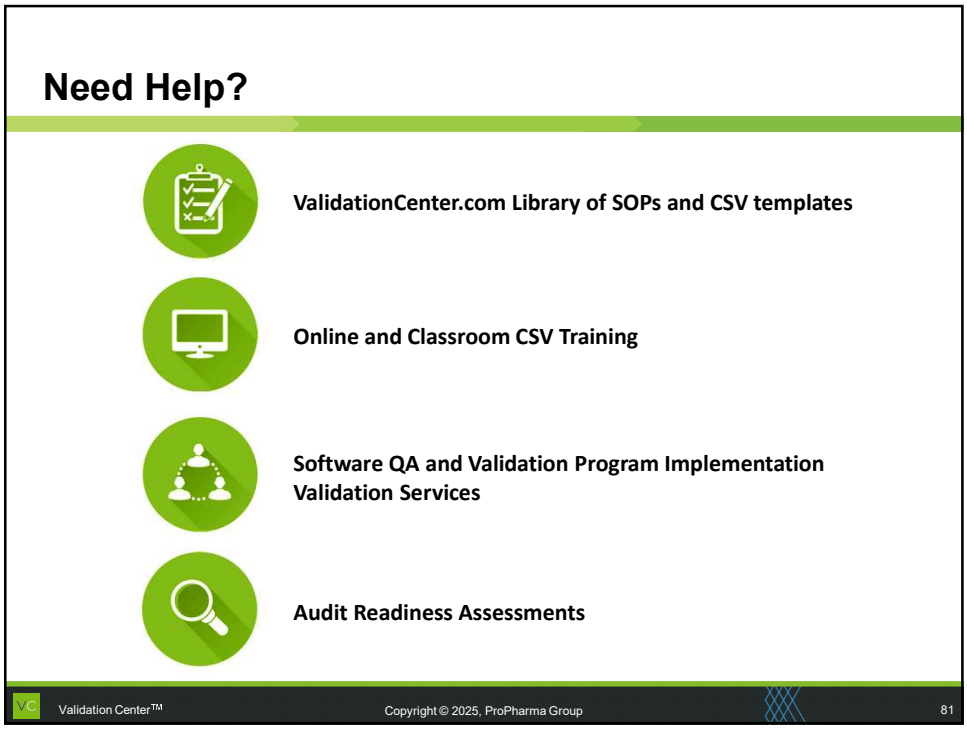
GMP	Good Manufacturing Practice
GCP	Good Clinical Practice
GLP	Good Laboratory Practice
GDP	Good Distribution Practice

Checklists

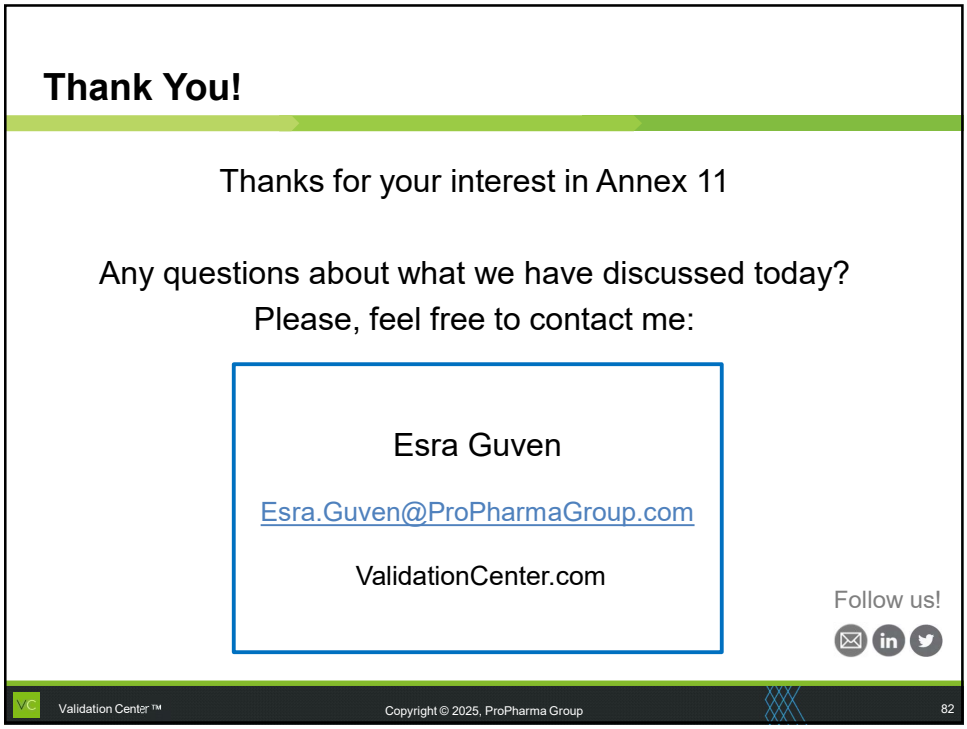
- Good Computer Validation Practices
- Computer System Validation Control Measures
- Requirements Inspection Points
- General Points for Inspectors to Consider
- User Responsibilities Points *from GAMP*

- Assurance of reliability of software is achieved by execution of quality plans and testing
- The regulated user's range of computerised systems needs to be formally listed in an inventory
- Changes to the validated computerised system require review and authorisation
- Access rights for all operators are clearly defined and controlled, including physical and logical access
- The validated back-up procedure including storage facilities and media should assure data integrity
- There should be special procedures for critical data entry requiring a second check
- Time-linked audit trail records should be available in a human readable form
- All staff who perform tasks associate with computerised systems must have requisite training
- It is essential for the regulated user to carry out a properly documented supplier assessment

80



81



82