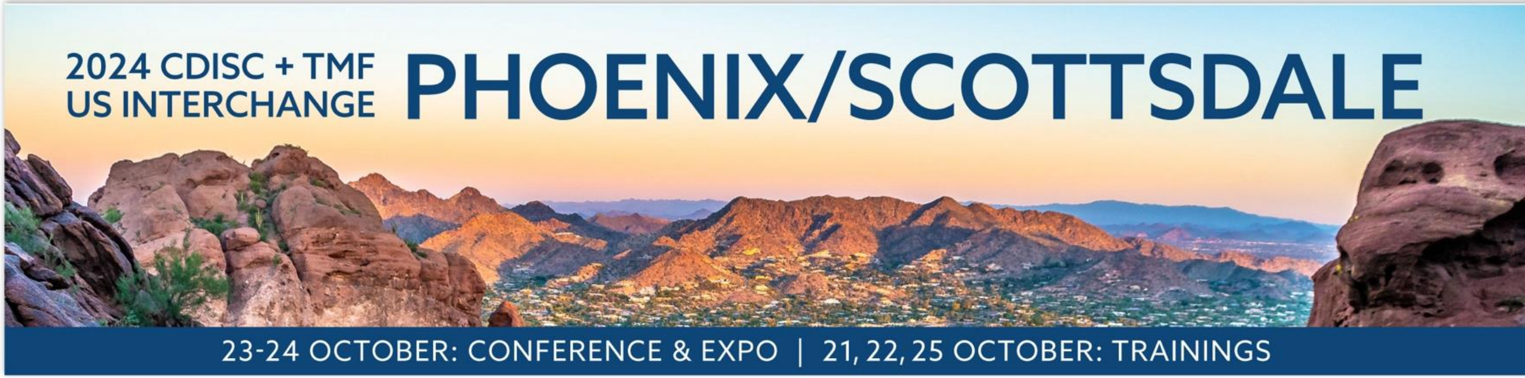
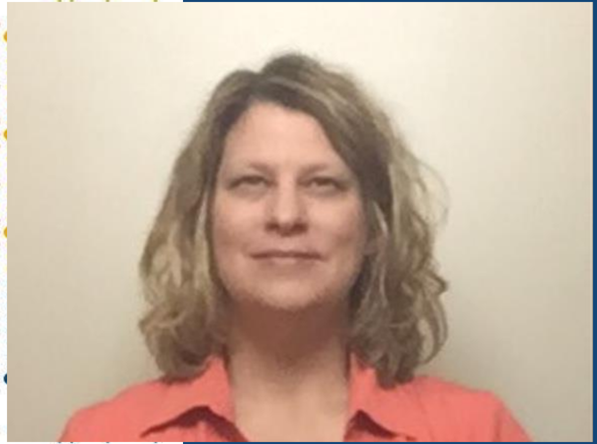

2024 CDISC + TMF
US INTERCHANGE
PHOENIX/SCOTTSDALE
23-24 OCTOBER: CONFERENCE & EXPO | 21, 22, 25 OCTOBER: TRAININGS

# The Requirements of the 2023 EMA Guideline on Clinical Systems and the CSV Tab of the CDSIC TMF RM

Presented by Lisa Dotterweich Mulcahy
Owner and Principal Consultant for Mulcahy Consulting



# Meet the Speaker

Lisa Dotterweich Mulcahy

Title: Owner and Principal Consultant

Organization: Mulcahy Consulting, LLC

Lisa Mulcahy has an extensive career in the biopharmaceutical industry in the areas of Clinical Operations, Quality Management, and TMF Management. She is an independent consultant for the last 17 years who ties previous work experiences together to assist clients to develop, revise, and operationalize high-quality and compliant TMFs and associated management processes to achieve complete and inspection-ready of TMFs and their long-term preservation.

Lisa is a co-founder, a current Steering Committee member of the CDISC TMF Reference Model volunteer team of industry representatives that created and maintain the model. She is co-lead of the CDISC TMF RM Education Governance Committee and part of the management team of TMF RM V4 Refresh project.

# Disclaimer and Disclosures

- *The views and opinions expressed in this presentation are those of the author and do not necessarily reflect the official policy or position of CDISC.*

- *The author has no real or apparent conflicts of interest to report.*

## Pre-Agenda

1. Quick Knowledge Check of Audience
2. Summary of this Presentation
3. 2018 EMA Guideline on the trial master file

# Quick Knowledge Check of Audience – Hands Up

## The TMF is comprised of multiple computerised systems

**Q.4** Who in this room recognized that the CSV tab was important to them as TMF management professionals? Who has used it?

**Q.1** Who in this room is really familiar with the 2018 EMA Guideline on content, management, and archiving of the clinical trial master file?

**Q.2** Who in this room is familiar with the 2023 EMA Guideline on content, management, and archiving of the clinical trial master file?  And?

**Q.3** Who in this room knows that there was a CSV tab in the TMF RM?

**Q.4** Who in this room recognized that the CSV tab was important to them as TMF management professionals? Who has used it?

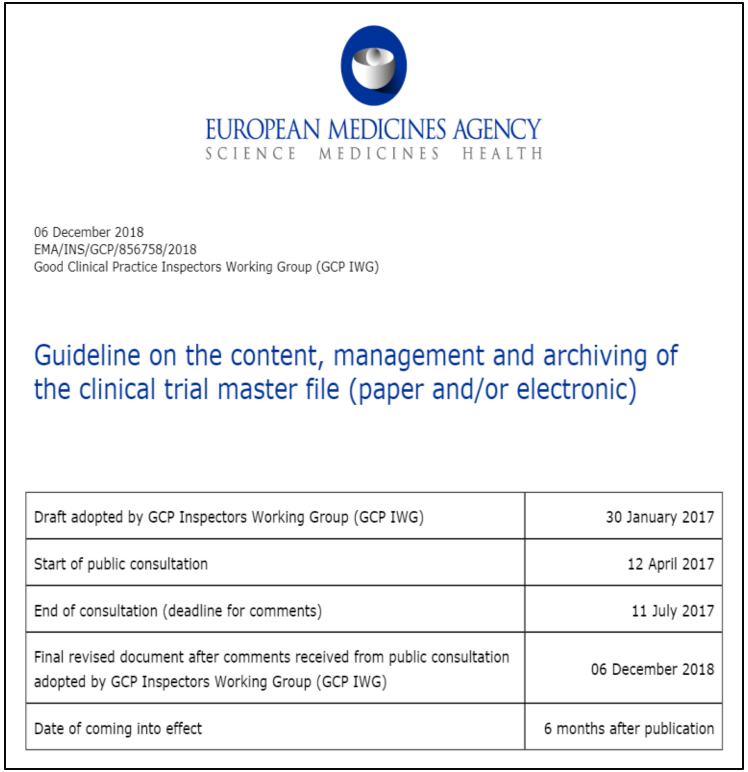
# Summary of this Presentation

The TMF for a clinical study can be maintained in a variety of computerised systems; each of them considered TMF repositories. TMF repositories are to be validated per the published EMA guideline titled “Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)” released in December 2018.

Since then, EMA GCP Inspectors Working Group published the “Guideline on computerised systems and electronic data in clinical trials” in March 2023, which became effective in September 2023, the oversight and assurance related documentation associated with all of the software as a service computerised systems utilized in clinical studies has been brought view, more so than ever before.

The artifacts listed in the TMF RM Computer System Validation (CSV) tab align very nicely with the expectations of the guideline. The future of the CSV tab is up for discussion during the TMF RM V4 Refresh project. This presentation will ask this audience their opinions to drive its future.

# The 2018 EMA Guideline on content, management, and archiving of the clinical trial master file



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

06 December 2018
EMA/INS/GCP/856758/2018
Good Clinical Practice Inspectors Working Group (GCP IWG)

Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)

| | |
|---|---|
| Draft adopted by GCP Inspectors Working Group (GCP IWG) | 30 January 2017 |
| Start of public consultation | 12 April 2017 |
| End of consultation (deadline for comments) | 11 July 2017 |
| Final revised document after comments received from public consultation adopted by GCP Inspectors Working Group (GCP IWG) | 06 December 2018 |
| Date of coming into effect | 6 months after publication |

Guideline EMA GCP Inspectors Working Group

Released 06 December 2018

Effective 06 June 2019

EMA/INS/GCP/856758/2018

Good Clinical Practice Inspectors Working Grp

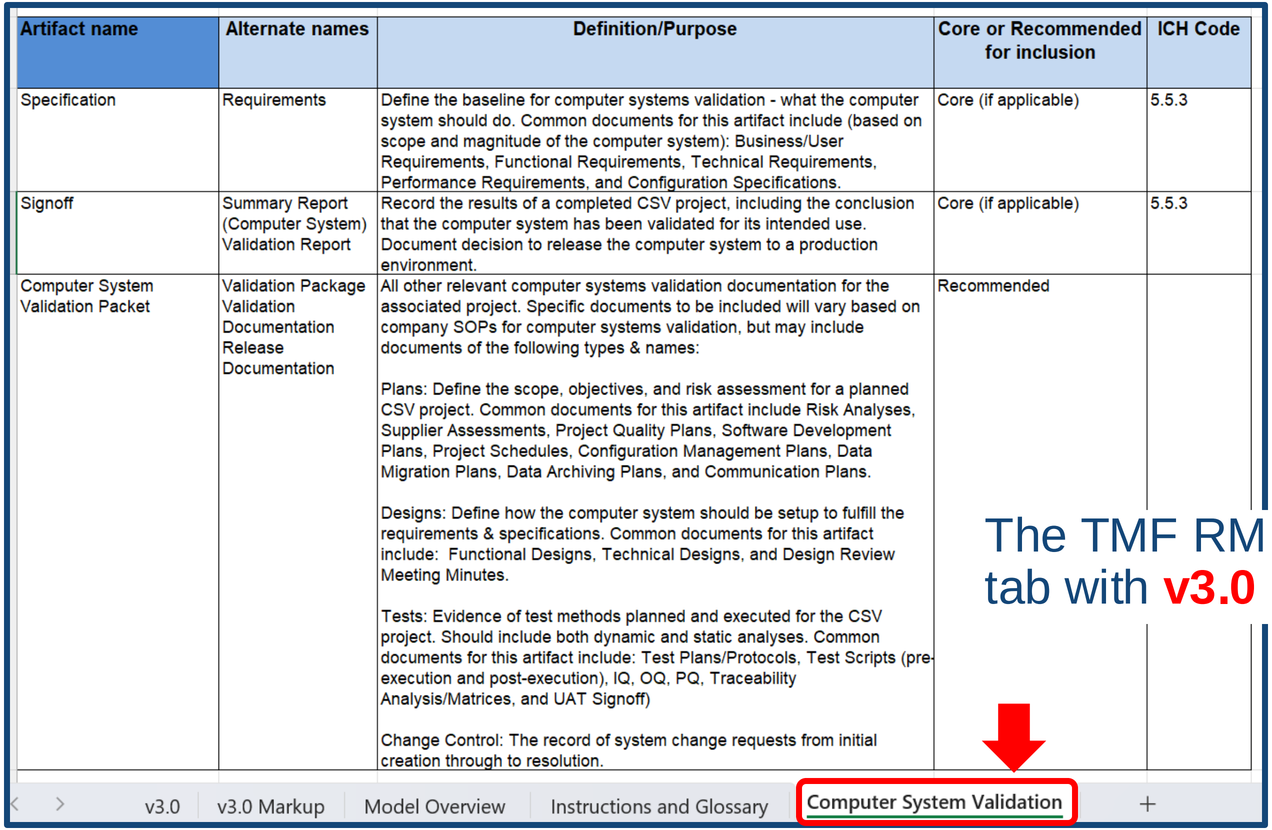
Guideline on the content, management and archiving of the clinical trial master file (paper and/or electronic)

> The systems *[that hold TMF records]* should be validated to demonstrate that the functionality is fit for purpose, with formal procedures in place to manage this process.

# Agenda

1. Computerised Systems – System-level v. Study-level
2. The CSV Tab of the TMF Reference Model
3. The 2023 EMA Guideline on Computerised Systems
   - Responsibilities for Oversight of Clinical Systems Utilized in Clinical Studies
   - Process and Resulting Evidence of Oversight
4. What might the CSV artifacts look like in TMF RM V4?
5. Thank you and Feedback

# The Trial Master File Reference Model – CSV Tab



| Artifact name | Alternate names | Definition/Purpose | Core or Recommended for inclusion | ICH Code |
|---|---|---|---|---|
| Specification | Requirements | Define the baseline for computer systems validation - what the computer system should do. Common documents for this artifact include (based on scope and magnitude of the computer system): Business/User Requirements, Functional Requirements, Technical Requirements, Performance Requirements, and Configuration Specifications. | Core (if applicable) | 5.5.3 |
| Signoff | Summary Report (Computer System) Validation Report | Record the results of a completed CSV project, including the conclusion that the computer system has been validated for its intended use. Document decision to release the computer system to a production environment. | Core (if applicable) | 5.5.3 |
| Computer System Validation Packet | Validation Package<br>Validation Documentation<br>Release Documentation | All other relevant computer systems validation documentation for the associated project. Specific documents to be included will vary based on company SOPs for computer systems validation, but may include documents of the following types & names:<br><br>Plans: Define the scope, objectives, and risk assessment for a planned CSV project. Common documents for this artifact include Risk Analyses, Supplier Assessments, Project Quality Plans, Software Development Plans, Project Schedules, Configuration Management Plans, Data Migration Plans, Data Archiving Plans, and Communication Plans.<br><br>Designs: Define how the computer system should be setup to fulfill the requirements & specifications. Common documents for this artifact include: Functional Designs, Technical Designs, and Design Review Meeting Minutes.<br><br>Tests: Evidence of test methods planned and executed for the CSV project. Should include both dynamic and static analyses. Common documents for this artifact include: Test Plans/Protocols, Test Scripts (pre-execution and post-execution), IQ, OQ, PQ, Traceability Analysis/Matrices, and UAT Signoff)<br><br>Change Control: The record of system change requests from initial creation through to resolution. | Recommended | |

The TMF RM added the tab with **v3.0** in June 2015.

# The Trial Master File Reference Model – CSV Tab

## Rationale

- The variety of computer systems utilized in execution of clinical trials continues to grow and includes both 'core' systems that are used for many trials and systems that are developed and/or configured for specific trials. ICH 5.5.3 suggests that when trial data handling systems are utilized, sponsors should complete computer systems validation (CSV) processes to "Ensure and document that the electronic data processing system(s) conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance."

# The Trial Master File Reference Model – CSV Tab

**Study-specific computerized systems or study-specific configurations**

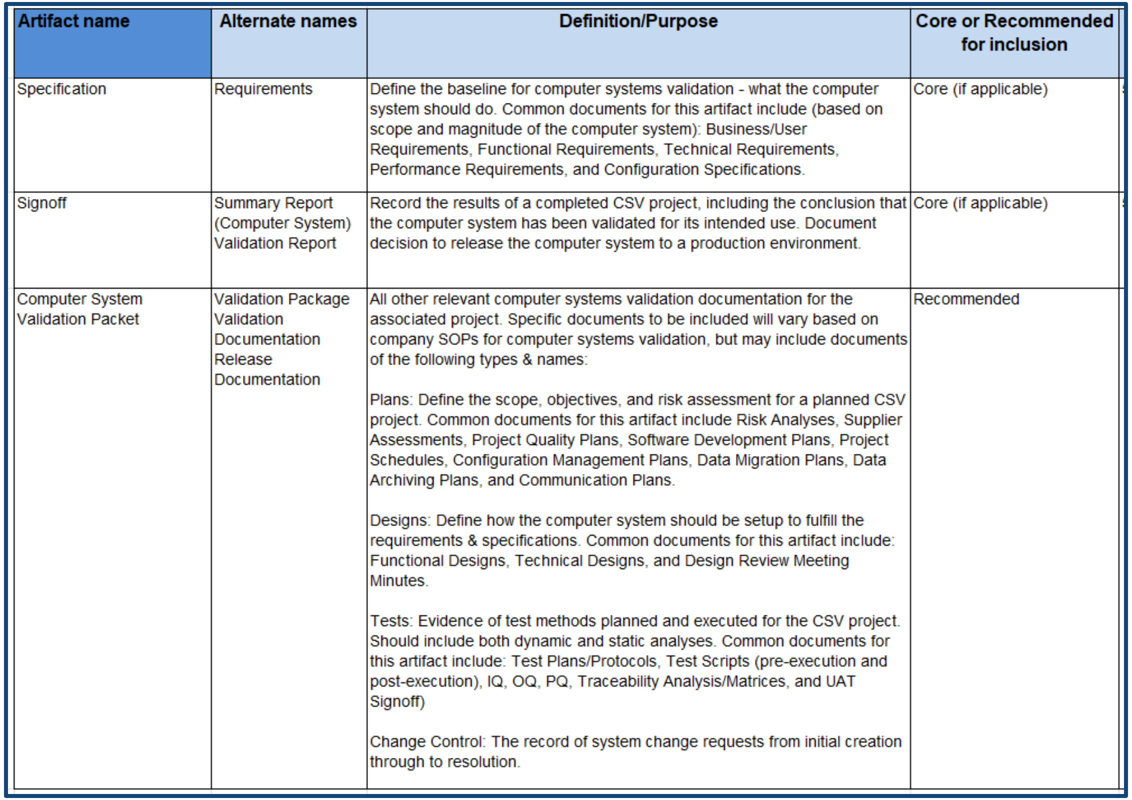
- The TMF Reference Model includes artifacts for IRT systems (Zone 6) and CDM/EDC systems (Zone 10). The CSV artifacts are not consistent between these two zones.
- In anticipation of new types of clinical study data systems and in order to more consistently account for CSV artifacts, a TMF Reference Model CSV tab has been included.
- This list is intended to include in scope only those computer systems which are specifically developed or configured to handle data and electronic records for a specific clinical study (for example, the computer systems development of most Clinical Trial Management Systems is not study-specific thus CTMS computer systems validation documentation would not be expected to be in scope).

# The Trial Master File Reference Model – CSV Tab

## Usage

- Use of these artifacts is strictly optional for the TMF Reference Model, either within zones or as a new zone - Zone 12 .
- An assessment has been completed and these artifacts will be maintained outside of the official TMF Reference Model. Your ongoing feedback & experience related to the classification of CSV artifacts is welcomed by the TMF Reference Model team.

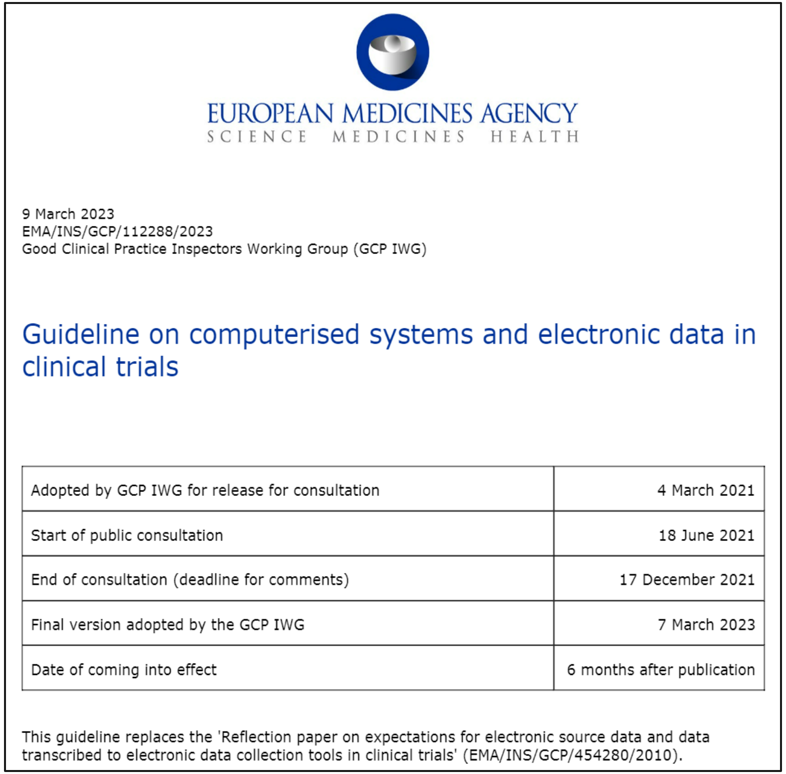
# The Trial Master File Reference Model – CSV Tab Artifacts



| Artifact name | Alternate names | Definition/Purpose | Core or Recommended for inclusion |
|---|---|---|---|
| Specification | Requirements | Define the baseline for computer systems validation - what the computer system should do. Common documents for this artifact include (based on scope and magnitude of the computer system): Business/User Requirements, Functional Requirements, Technical Requirements, Performance Requirements, and Configuration Specifications. | Core (if applicable) |
| Signoff | Summary Report<br>(Computer System) Validation Report | Record the results of a completed CSV project, including the conclusion that the computer system has been validated for its intended use. Document decision to release the computer system to a production environment. | Core (if applicable) |
| Computer System Validation Packet | Validation Package<br>Validation Documentation<br>Release Documentation | All other relevant computer systems validation documentation for the associated project. Specific documents to be included will vary based on company SOPs for computer systems validation, but may include documents of the following types & names:<br>Plans: Define the scope, objectives, and risk assessment for a planned CSV project. Common documents for this artifact include Risk Analyses, Supplier Assessments, Project Quality Plans, Software Development Plans, Project Schedules, Configuration Management Plans, Data Migration Plans, Data Archiving Plans, and Communication Plans.<br>Designs: Define how the computer system should be setup to fulfill the requirements & specifications. Common documents for this artifact include: Functional Designs, Technical Designs, and Design Review Meeting Minutes.<br>Tests: Evidence of test methods planned and executed for the CSV project. Should include both dynamic and static analyses. Common documents for this artifact include: Test Plans/Protocols, Test Scripts (pre-execution and post-execution), IQ, OQ, PQ, Traceability Analysis/Matrices, and UAT Signoff)<br>Change Control: The record of system change requests from initial creation through to resolution. | Recommended |

This tab compiles the full set of computer system validation documentation that would be required to be created for sponsor/ vendor-owned computerized systems, or the systems owned by the technical vendors who sell software as a service technology to sponsors utilized in a clinical study.

# The 2023 EMA Guideline on computerised systems and electronic data in clinical trials



EUROPEAN MEDICINES AGENCY
SCIENCE MEDICINES HEALTH

9 March 2023
EMA/INS/GCP/112288/2023
Good Clinical Practice Inspectors Working Group (GCP IWG)

Guideline on computerised systems and electronic data in clinical trials

| | |
|---|---|
| Adopted by GCP IWG for release for consultation | 4 March 2021 |
| Start of public consultation | 18 June 2021 |
| End of consultation (deadline for comments) | 17 December 2021 |
| Final version adopted by the GCP IWG | 7 March 2023 |
| Date of coming into effect | 6 months after publication |

This guideline replaces the 'Reflection paper on expectations for electronic source data and data transcribed to electronic data collection tools in clinical trials' (EMA/INS/GCP/454280/2010).

Guideline EMA GCP Inspectors Working Group

Released 09 March 2023

Effective 09 September 2023

EMA/INS/GCP/112288/2023

Good Clinical Practice Inspectors Working Grp

Guideline on computerized systems and electronic data in clinical trials

…'data' will be used in this guideline in a broad meaning, which may include documents, records or any form of information.

# The 2023 EMA Guidance on Computerised Systems

Unless otherwise specified (e.g. 'source data' or 'source document') and in order to simplify the text, **'data' will be used in this guideline in a broad meaning, which may include documents, records or any form of information.**

It covers requirements and expectations for computerized systems including validation, user management, security, and electronic data for the data life cycle.

The scope of this guideline is computerised systems, (including instruments, software and 'as a service') used in the creation/ capture of electronic clinical data and to the control of other processes with the potential to affect participant protection and reliability of trial data, in the conduct of a clinical trial of investigational medicinal products (IMPs).

These include but may not be limited to the following: EMR, Investigator tools, participant wearables, eCRFs, Temptales, scans/imaging, eTMFs, eICF, IRT, CTMS, Site Portals, safety database, remote monitoring. AI used in clinical trials, and other computerised systems implemented by the sponsor holding/ managing and/or analysing or reporting data relevant to the clinical trial e.g., clinical trial management systems (CTMS), pharmaco-vigilance databases, statistical software, document management systems, test management systems, and central monitoring software.

# The 2023 EMA Guideline on computerised systems and electronic Clinical Systems – Validation of systems

### *4.10. Validation of systems*

- Computerised systems used within a clinical trial should be subject to processes that confirm that the specified requirements of a computerised system are consistently fulfilled, and that the system is fit for purpose. Validation should ensure accuracy, reliability, and consistent intended performance, from the design until the decommissioning of the system or transition to a new system.
- The processes used for the validation should be decided upon by the system owner (e.g. sponsors, investigators, technical facilities) and described, as applicable. System owners should ensure adequate oversight of validation activities (and associated records) performed by service providers to ensure suitable procedures are in place and that they are being adhered to.
- Documentation (including information within computerised systems used as process tools for validation activities) should be maintained to demonstrate that the system is maintained in the validated state. Such documentation should be available for both the validation of the computerised system and for the validation of the trial specific configuration or customisation.
- Validation of the trial specific configuration or customisation should ensure that the system is consistent with the requirements of the approved clinical trial protocol and that robust testing of functionality implementing such requirements is undertaken, for example, eligibility criteria questions in an eCRF, randomisation strata and dose calculations in an IRT system.

# Annex 2 – Computerised system validation

The responsible party should ensure that systems used in clinical trials have been appropriately validated

The responsible party may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate

The responsible party may also have to perform additional validation activities based on a documented assessment or their processes.

In any case, the responsible party remains ultimately responsible for the validation of the computerised systems used in clinical trials.

If the responsible party wants to use the vendor's validation documentation, they should ensure that it covers their intended use as well as its defined needs and requirements through audit.

In case the vendor’s validation activities and documentation are insufficient … the responsible party should validate the system.

New functionalities should not be used by the responsible party until they have validated them or reviewed and assessed the vendor's documentation.

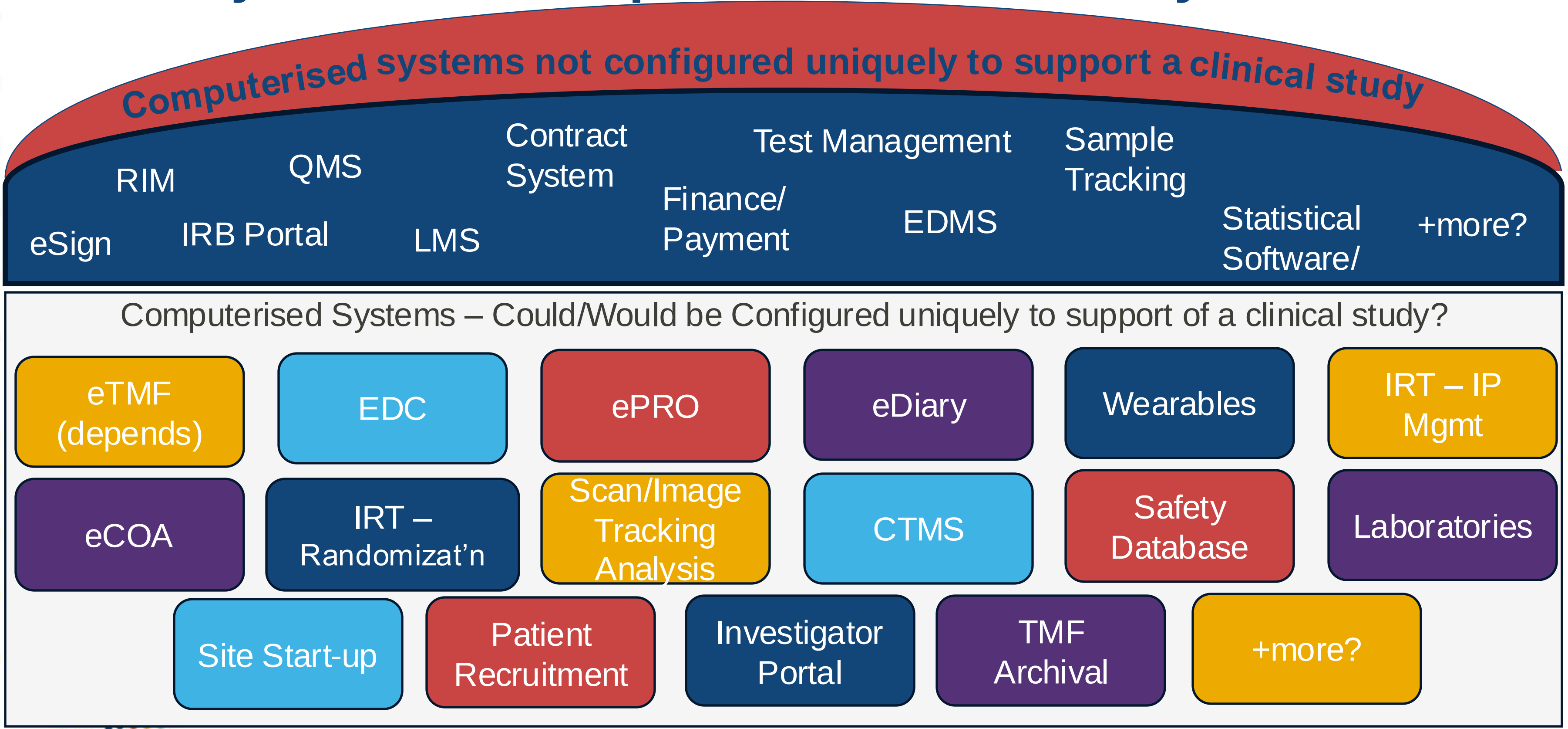
Critical system functionality implemented and used in a clinical trial should be described in a set of user requirements, tested, reported on before release

Prior to testing, the risk assessment should define which requirements and tests are related to critical system functionality.

# Responsibilities for Oversight of Clinical Systems Utilized in Clinical Studies

- Oversight
  - Each responsible party is responsible for oversight of the technical vendor and the software they provide.  (I personally call this assurance)
  - Each responsible party needs to defines their intended level of oversight of a computerized system used in a clinical study and it based on audit of the technical vendors validation related processes and resultant documentation.  This documented in processes.
  - Specifications for configurations made to system to meet responsible party's defined critical functionalities and study-specific needs (fit for purpose) are documented in a user requirement specification document
- Evidence of Oversight
  - Audit report (including any completed CAPAs) of technical vendor to review system level validation process and produced records
  - Review of specific validation-related records created by the technical vendor for the software
  - Assessment (including risk assessment) of new or updated functionalities consider to be critical by the responsible party
  - Creation of the assurance related records according the established process

# Computerised systems and electronic Clinical Systems – Enterprise Level and Study Level



Computerised systems not configured uniquely to support a *clinical study*

RIM

QMS

Contract System

Test Management

Sample Tracking

eSign

IRB Portal

LMS

Finance/ Payment

EDMS

Statistical Software/

+more?

Computerised Systems – Could/Would be Configured uniquely to support of a clinical study?

eTMF (depends)

EDC

ePRO

eDiary

Wearables

IRT – IP Mgmt

eCOA

IRT – Randomizat'n

Scan/Image Tracking Analysis

CTMS

Safety Database

Laboratories

Site Start-up

Patient Recruitment

Investigator Portal

TMF Archival

+more?

Does a company have to duplicate the CSV related activities that were performed by the technology vendor?

It depends.  Not duplicate if the company performed audit of vendor and the vendor passed the audit and the company determined the vendor has adequate process and documentation.

If a software as a service technology is purchased, does this make a difference?

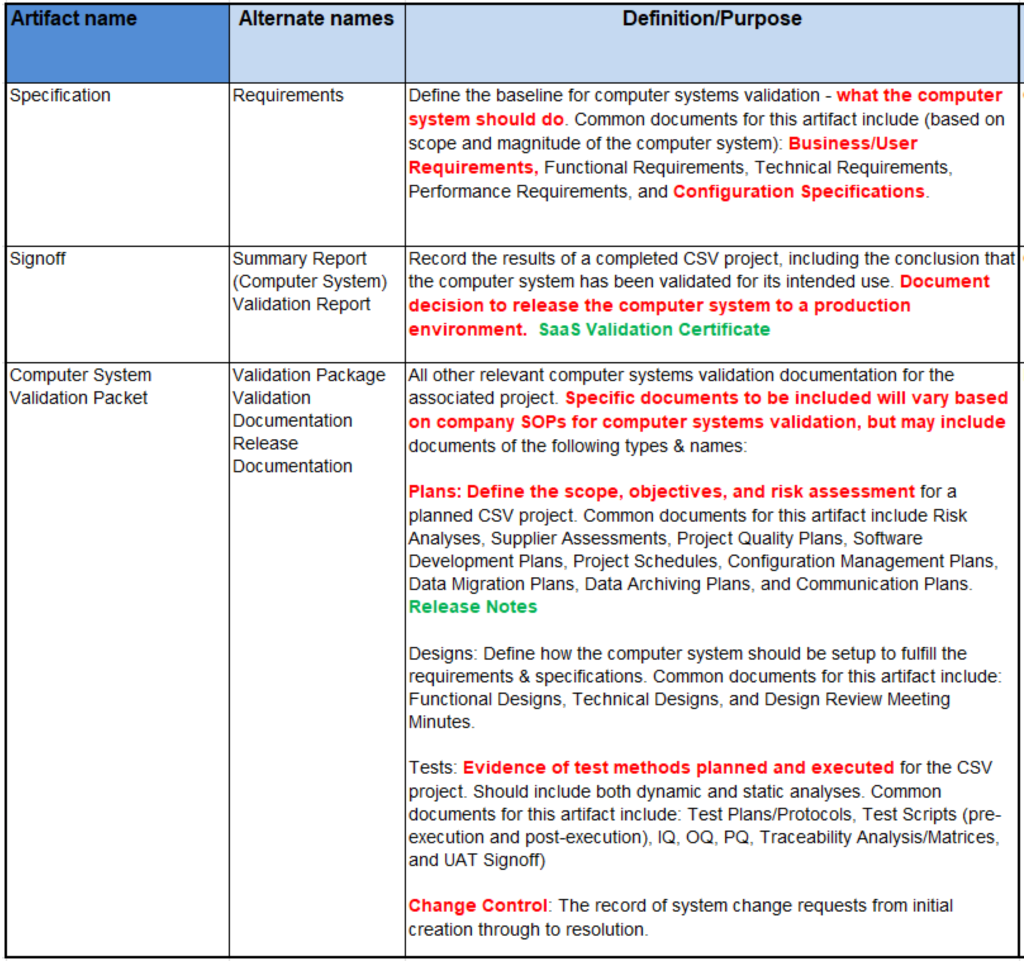
Assuming the vendor passed the audit, duplication is not required. It is about defining a CSV assurance process (functional/user requirements, risk assessment, plans, testing requirements, reports)

Are there differences in the responsible party’s obligations for the enterprise level systems versus computerised system used in clinical studies?

Where is the CSV-related documentation maintained for enterprise level computerized systems? What about for computerised system used in clinical studies?

If the repository holds TMF records, then the system needs to be validated and oversight performed

Enterprise Level: Company repository such as QMS.
Study–specific: TMF



| Artifact name | Alternate names | Definition/Purpose |
|---|---|---|
| Specification | Requirements | Define the baseline for computer systems validation - **what the computer system should do**. Common documents for this artifact include (based on scope and magnitude of the computer system): **Business/User Requirements,** Functional Requirements, Technical Requirements, Performance Requirements, and **Configuration Specifications**. |
| Signoff | Summary Report (Computer System) Validation Report | Record the results of a completed CSV project, including the conclusion that the computer system has been validated for its intended use. **Document decision to release the computer system to a production environment.** **SaaS Validation Certificate** |
| Computer System Validation Packet | Validation Package<br>Validation Documentation<br>Release Documentation | All other relevant computer systems validation documentation for the associated project. **Specific documents to be included will vary based on company SOPs for computer systems validation, but may include** documents of the following types & names:<br>**Plans: Define the scope, objectives, and risk assessment** for a planned CSV project. Common documents for this artifact include Risk Analyses, Supplier Assessments, Project Quality Plans, Software Development Plans, Project Schedules, Configuration Management Plans, Data Migration Plans, Data Archiving Plans, and Communication Plans. **Release Notes**<br>Designs: Define how the computer system should be setup to fulfill the requirements & specifications. Common documents for this artifact include: Functional Designs, Technical Designs, and Design Review Meeting Minutes.<br>Tests: **Evidence of test methods planned and executed** for the CSV project. Should include both dynamic and static analyses. Common documents for this artifact include: Test Plans/Protocols, Test Scripts (pre-execution and post-execution), IQ, OQ, PQ, Traceability Analysis/Matrices, and UAT Signoff)<br>**Change Control**: The record of system change requests from initial creation through to resolution. |

# What might be included in a **CSV Assurance Process** for a system which passed an audit by responsible party?

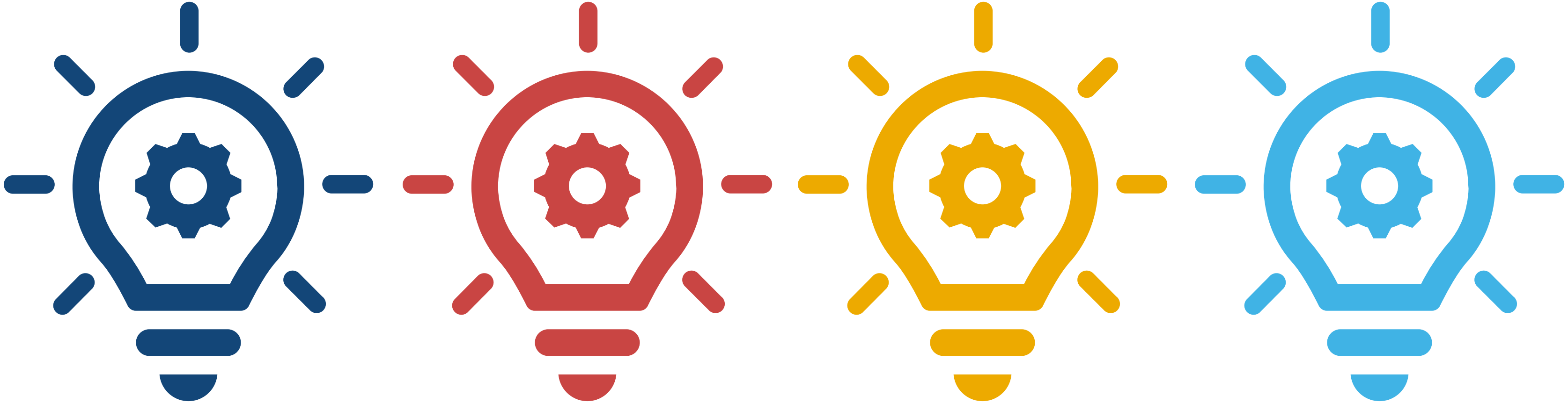
- Change Control
- Business/User/Functional Specifications
  - Definition of critical functionality
  - Configuration specifications
- Release Notes
- Risk Assessment
- Plan for testing
- Testing related records
- Report
- System’s Validation Certificate

**!! Remember to Define, identify risks, prepare to defend decisions**

# Will the CSV Tab Exist in V4 of the TMF RM?

The TMF RM V4 team is assembling a working group to tackle this question.

What are your thoughts on how the CSV related records for the **computerised systems used in clinical studies.**



# Thank you and Your Thoughts on the Topic

- Thanks to YOU for attending this session.
- Thanks to CDSIC for the support of the TMF RM
- Thanks to the 2024 CDISC+TMF US Interchange Planning Committee for all the support that they provided me to speak to you today

- If you have more thoughts on this topic, please provide to me your thoughts and comments on this topic.
  - Talk to me in person after this session, at breaks, during lunches, and even after the meeting by emailing me at lisa.mulcahy@mcllc-tmf.com
  - Let me know if you think that additional industry learning opportunities, for example a 2-hour training course to take a deeper dive into CSV related documentation/records, is a worthwhile effort?

# Back-up slides

# The 2023 EMA Guideline on computerised systems and electronic Clinical Systems – Cloud Solutions

## *6.7 - Cloud Solutions*

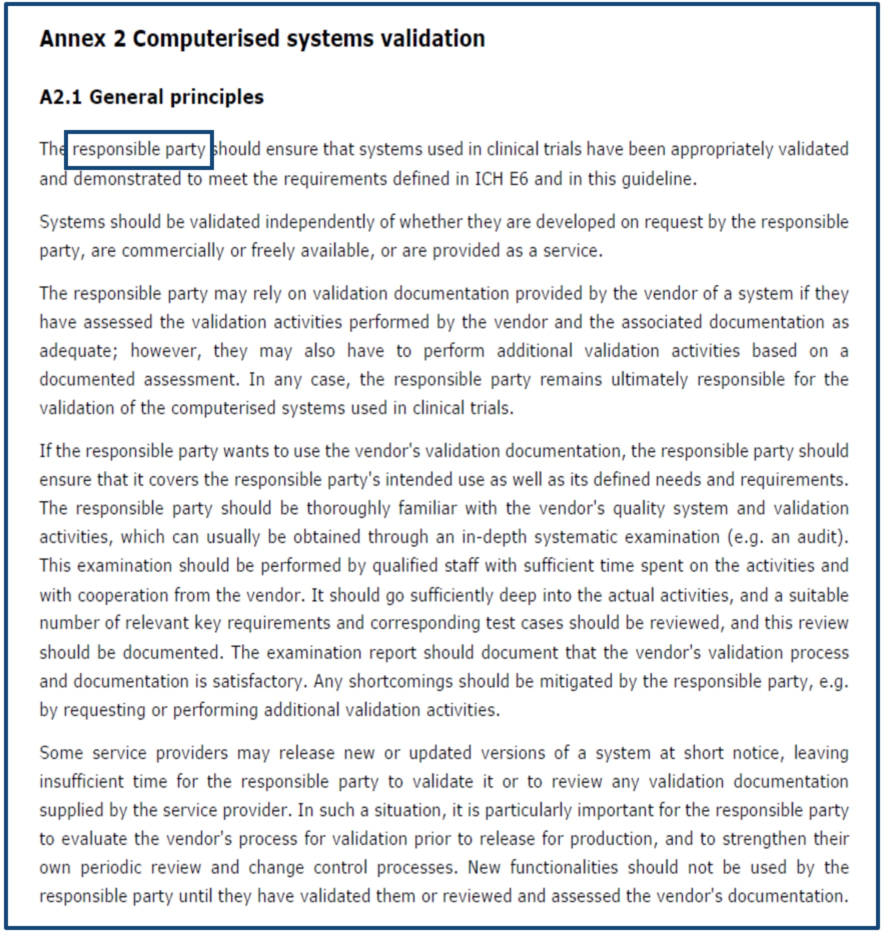
- Irrespective whether a computerised system is installed at the premises of the sponsor, investigator, another party involved in the trial or whether it is made available by a service provider as a cloud solution, the requirements in this guideline are applicable. There are, however, specific points to be considered as described below.
- Cloud solutions cover a wide variety of services related to the computerised systems used in clinical trials. These can range from Infrastructure as a Service (IaaS) over Platform as a Service (PaaS) to **Software as a Service (SaaS)**. It is common for these services that they provide the responsible party on-demand availability of computerised system resources over the internet, without having the need or even the possibility to directly manage these services.
- If the responsible party choses to perform their own validation of the computerised system, the cloud provider should make a test environment available that is identical to the production environment.

# Annex 2
# 2.1 – General Principles

The responsible party should ensure that systems used in clinical trials have been appropriately validated and demonstrated to meet the requirements defined in ICH E6 and in this guideline.

The responsible party may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate;

however, they may also have to perform additional validation activities based on a documented assessment. In any case, the responsible party remains ultimately responsible for the validation of the computerised systems used in clinical trials.



## Annex 2 Computerised systems validation

### A2.1 General principles

The responsible party should ensure that systems used in clinical trials have been appropriately validated and demonstrated to meet the requirements defined in ICH E6 and in this guideline.

Systems should be validated independently of whether they are developed on request by the responsible party, are commercially or freely available, or are provided as a service.

The responsible party may rely on validation documentation provided by the vendor of a system if they have assessed the validation activities performed by the vendor and the associated documentation as adequate; however, they may also have to perform additional validation activities based on a documented assessment. In any case, the responsible party remains ultimately responsible for the validation of the computerised systems used in clinical trials.

If the responsible party wants to use the vendor's validation documentation, the responsible party should ensure that it covers the responsible party's intended use as well as its defined needs and requirements. The responsible party should be thoroughly familiar with the vendor's quality system and validation activities, which can usually be obtained through an in-depth systematic examination (e.g. an audit). This examination should be performed by qualified staff with sufficient time spent on the activities and with cooperation from the vendor. It should go sufficiently deep into the actual activities, and a suitable number of relevant key requirements and corresponding test cases should be reviewed, and this review should be documented. The examination report should document that the vendor's validation process and documentation is satisfactory. Any shortcomings should be mitigated by the responsible party, e.g. by requesting or performing additional validation activities.

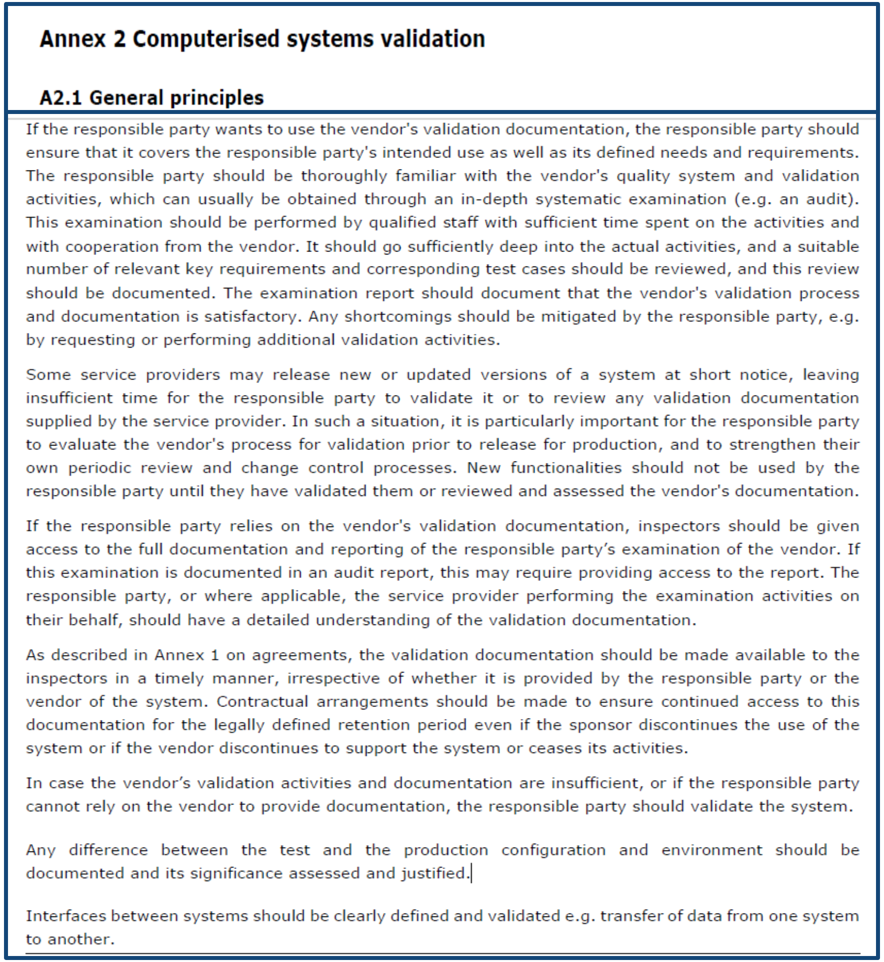
Some service providers may release new or updated versions of a system at short notice, leaving insufficient time for the responsible party to validate it or to review any validation documentation supplied by the service provider. In such a situation, it is particularly important for the responsible party to evaluate the vendor's process for validation prior to release for production, and to strengthen their own periodic review and change control processes. New functionalities should not be used by the responsible party until they have validated them or reviewed and assessed the vendor's documentation.

# Annex 2
# 2.1 – General Principles

If the responsible party wants to use the vendor's validation documentation, the responsible party should ensure that it covers the responsible party's intended use as well as its defined needs and requirements. The responsible party should be thoroughly familiar with the vendor's quality system and validation activities, which can usually be obtained through an in-depth systematic examination (e.g., an audit). The examination report should document that the vendor's validation process and documentation is satisfactory.

New functionalities should not be used by the responsible party until they have validated them or reviewed and assessed the vendor's documentation.

In case the vendor’s validation activities and documentation are insufficient … the responsible party should validate the system.



**Annex 2 Computerised systems validation**

**A2.1 General principles**

If the responsible party wants to use the vendor's validation documentation, the responsible party should ensure that it covers the responsible party's intended use as well as its defined needs and requirements. The responsible party should be thoroughly familiar with the vendor's quality system and validation activities, which can usually be obtained through an in-depth systematic examination (e.g. an audit). This examination should be performed by qualified staff with sufficient time spent on the activities and with cooperation from the vendor. It should go sufficiently deep into the actual activities, and a suitable number of relevant key requirements and corresponding test cases should be reviewed, and this review should be documented. The examination report should document that the vendor's validation process and documentation is satisfactory. Any shortcomings should be mitigated by the responsible party, e.g. by requesting or performing additional validation activities.

Some service providers may release new or updated versions of a system at short notice, leaving insufficient time for the responsible party to validate it or to review any validation documentation supplied by the service provider. In such a situation, it is particularly important for the responsible party to evaluate the vendor's process for validation prior to release for production, and to strengthen their own periodic review and change control processes. New functionalities should not be used by the responsible party until they have validated them or reviewed and assessed the vendor's documentation.

If the responsible party relies on the vendor's validation documentation, inspectors should be given access to the full documentation and reporting of the responsible party’s examination of the vendor. If this examination is documented in an audit report, this may require providing access to the report. The responsible party, or where applicable, the service provider performing the examination activities on their behalf, should have a detailed understanding of the validation documentation.

As described in Annex 1 on agreements, the validation documentation should be made available to the inspectors in a timely manner, irrespective of whether it is provided by the responsible party or the vendor of the system. Contractual arrangements should be made to ensure continued access to this documentation for the legally defined retention period even if the sponsor discontinues the use of the system or if the vendor discontinues to support the system or ceases its activities.

In case the vendor’s validation activities and documentation are insufficient, or if the responsible party cannot rely on the vendor to provide documentation, the responsible party should validate the system.

Any difference between the test and the production configuration and environment should be documented and its significance assessed and justified.

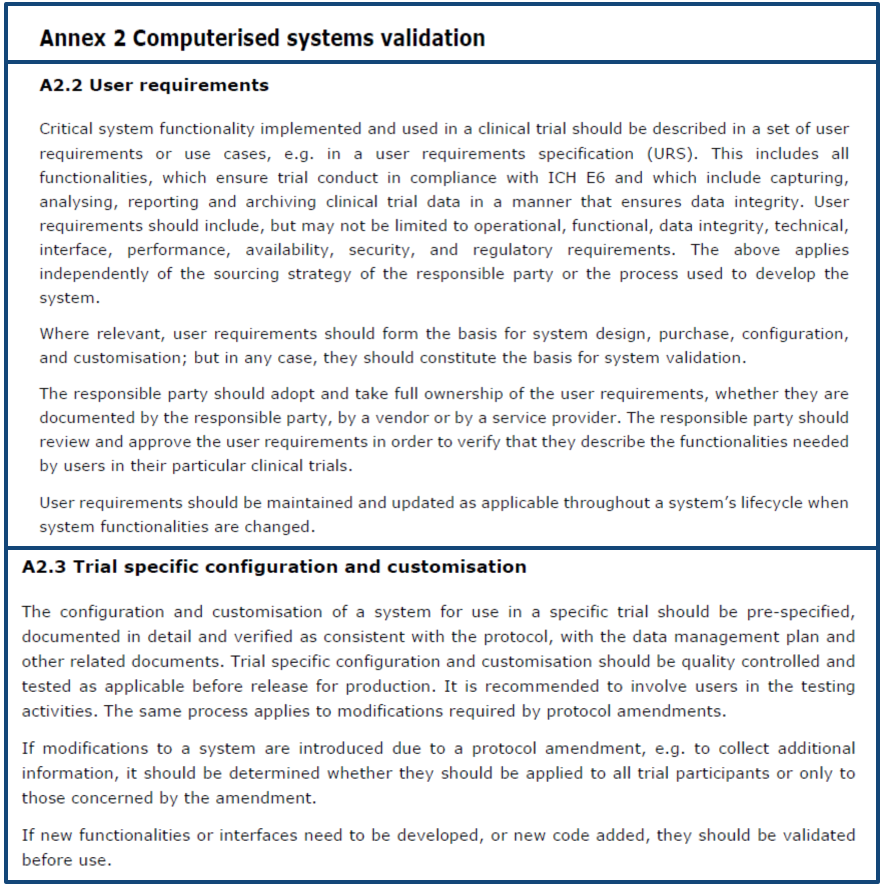
Interfaces between systems should be clearly defined and validated e.g. transfer of data from one system to another.

# Annex 2
# 2.2 – User Requirements
# 2.3 – Trial Specific Config

Critical system functionality implemented and used in a clinical trial should be described in a set of user requirements or use cases, e.g. in a user requirements specification (URS).

The responsible party should adopt and take full ownership of the user requirements, whether they are documented by the responsible party, by a vendor or by a service provider. The responsible party should review and approve the user requirements in order to verify that they describe the functionalities needed by users in their particular clinical trials.

Trial specific configuration and customisation should be quality controlled and tested as applicable before release for production. It is recommended to involve users in the testing activities.



**Annex 2 Computerised systems validation**

**A2.2 User requirements**

Critical system functionality implemented and used in a clinical trial should be described in a set of user requirements or use cases, e.g. in a user requirements specification (URS). This includes all functionalities, which ensure trial conduct in compliance with ICH E6 and which include capturing, analysing, reporting and archiving clinical trial data in a manner that ensures data integrity. User requirements should include, but may not be limited to operational, functional, data integrity, technical, interface, performance, availability, security, and regulatory requirements. The above applies independently of the sourcing strategy of the responsible party or the process used to develop the system.

Where relevant, user requirements should form the basis for system design, purchase, configuration, and customisation; but in any case, they should constitute the basis for system validation.

The responsible party should adopt and take full ownership of the user requirements, whether they are documented by the responsible party, by a vendor or by a service provider. The responsible party should review and approve the user requirements in order to verify that they describe the functionalities needed by users in their particular clinical trials.

User requirements should be maintained and updated as applicable throughout a system's lifecycle when system functionalities are changed.

**A2.3 Trial specific configuration and customisation**

The configuration and customisation of a system for use in a specific trial should be pre-specified, documented in detail and verified as consistent with the protocol, with the data management plan and other related documents. Trial specific configuration and customisation should be quality controlled and tested as applicable before release for production. It is recommended to involve users in the testing activities. The same process applies to modifications required by protocol amendments.

If modifications to a system are introduced due to a protocol amendment, e.g. to collect additional information, it should be determined whether they should be applied to all trial participants or only to those concerned by the amendment.

If new functionalities or interfaces need to be developed, or new code added, they should be validated before use.

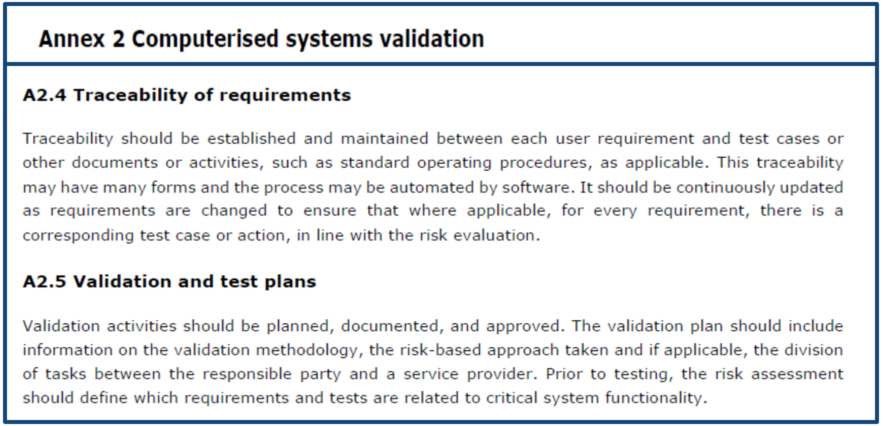
# Annex 2
# 2.4 – Traceability
# 2.5 – Validation and test plans
# 2.6 – Test Execution and Reporting

*(Traceability is documented if responsibility party is performing full validation)*

Validation activities should be planned, documented, and approved. Prior to testing, the risk assessment should define which requirements and tests are related to critical system functionality.

Testing … may even allow automatic execution of test cases (e.g. regression testing).

Test execution should follow approved protocols, documented, and a validation report approved by responsible party. The responsible party should sign off the release of the system.



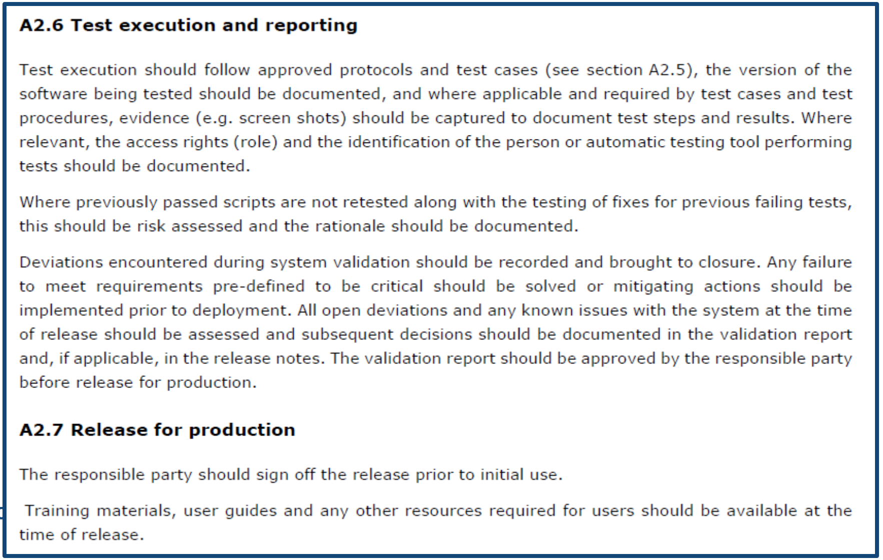
### Annex 2 Computerised systems validation

**A2.4 Traceability of requirements**

Traceability should be established and maintained between each user requirement and test cases or other documents or activities, such as standard operating procedures, as applicable. This traceability may have many forms and the process may be automated by software. It should be continuously updated as requirements are changed to ensure that where applicable, for every requirement, there is a corresponding test case or action, in line with the risk evaluation.

**A2.5 Validation and test plans**

Validation activities should be planned, documented, and approved. The validation plan should include information on the validation methodology, the risk-based approach taken and if applicable, the division of tasks between the responsible party and a service provider. Prior to testing, the risk assessment should define which requirements and tests are related to critical system functionality.



**A2.6 Test execution and reporting**

Test execution should follow approved protocols and test cases (see section A2.5), the version of the software being tested should be documented, and where applicable and required by test cases and test procedures, evidence (e.g. screen shots) should be captured to document test steps and results. Where relevant, the access rights (role) and the identification of the person or automatic testing tool performing tests should be documented.

Where previously passed scripts are not retested along with the testing of fixes for previous failing tests, this should be risk assessed and the rationale should be documented.

Deviations encountered during system validation should be recorded and brought to closure. Any failure to meet requirements pre-defined to be critical should be solved or mitigating actions should be implemented prior to deployment. All open deviations and any known issues with the system at the time of release should be assessed and subsequent decisions should be documented in the validation report and, if applicable, in the release notes. The validation report should be approved by the responsible party before release for production.

**A2.7 Release for production**

The responsible party should sign off the release prior to initial use.

Training materials, user guides and any other resources required for users should be available at the time of release.

# Regression Testing

Regression testing is a type of QA software testing that ensures changes or updates to an existing software product do not affect previously functioning features.
This type of testing may be necessary following various changes, including:

- Bug fixes
- Software enhancements
- Configuration adjustments, and
- Even the substitution of electronic components (hardware).

A regression test asks, "Does everything still work as expected?" A malfunction or bug in another part of the system caused by a new release is called a "regression," hence the term "regression testing."

Regression testing encompasses a broad spectrum of testing methodologies, such as functional testing, performance testing, and security testing. Additionally, it involves examining integrations among different software components and validating data migration between systems

https://www.globalapptesting.com/regression-testing-guide#:~:text=Regression%20testing%20is%20a%20type,Configuration%20adjustments%2C%20and

Could Regression Testing be Used as a testing method for assessing new or updated clinical system functionalities?

This depends on the responsible party's defined process for assurance.