



2025

CDISC + TMF
EUROPE INTERCHANGE

GENEVA

CONFERENCE & EXPO: 14-15 MAY | TRAININGS: 12, 13, 16 MAY

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

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

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 on the Project Management Team, co-leading the Triage Committee, working on the update of the TMF RM to V4.0.

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.*

Quick Knowledge Check of Audience – Hands Up

The TMF is comprised of multiple computerised systems

Q.6 Who in this room does oversight of the software as a service clinical system to ensure it remains fit for purpose after upgrades?



Q.1 Who in this room is 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 computerised systems and electronic data in clinical trials?

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

Q.5 Who in this room uses a software as a service clinical system in their clinical studies or to manage TMF records?

Q.6 Who in this room does oversight of the software as a service clinical system to ensure it remains fit for purpose after upgrades?

Have You Experienced this Range of Emotions after a Clinical System Upgrade when You Find a System Issue?



Yay!
Cannot wait to try new or improved system features and functionalities



Wait!
Something just isn't right. System is not working as it should.



Oh no!
I cannot do my job (or some portion of my job)



Errrr!
System not as expected. Why doesn't technical vendor know there is an issue?



Wah!
What else is not working? How long will this last?



Now an informal case study to share

Oversight of system upgrades and testing of your system's critical functionalities give confidence that system working as it should and if not, it would let you know issues, report them, and get them addressed quicker.

Key Points to Presentation

TMF records 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, EMA guidance released in March of 2023, and ICH GCP R3 released in January 2025.

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 into view, more so than ever.

The artifacts listed in the TMF RM **Computer System Validation (CSV) tab** align very nicely with the expectations of the guideline. Variances are for system level or study-specific configurations.

Records in the CSV tab will be **incorporated into the TMF RM V4**.
How is still to be determined... a work group has been formed on this topic.

Computerised Clinical Systems

-Enterprise/System Level and Study Level-

- TMF Repositories
- Validated
- Oversight and Assurance
- TMF RM CVA Artifacts
- TMF RM V4

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?



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

- TMF Repositories
- **Validated**
- Oversight and Assurance
- TMF RM CVA Artifacts
- TMF RM V4



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.


* Text not in the guidance language

The Trial Master File Reference Model – Computer System Validation Tab

- TMF Repositories
- Validated
- **TMF RM CSV Artifacts**
- Oversight and Assurance
- TMF RM V4

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 Validation Documentation Release Documentation	<p>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:</p> <p>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.</p> <p>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.</p> <p>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)</p> <p>Change Control: The record of system change requests from initial creation through to resolution.</p>	Recommended	

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



< > v3.0 v3.0 Markup Model Overview Instructions and Glossary Computer System Validation +

The Trial Master File Reference Model – Computer System Validation Tab


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 (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 Validation Documentation Release Documentation	<p>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:</p> <p>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.</p> <p>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.</p> <p>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)</p> <p>Change Control: The record of system change requests from initial creation through to resolution.</p>	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.

Review the definitions to get a comprehensive listing.

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

- TMF Repositories
- Validated
- TMF RM CSV Artifacts
- **Oversight and Assurance**
- TMF RM V4



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 ... 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 data in clinical systems–Validation of systems

4.10. *Validation of systems*

- 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.



The 2023 EMA Guideline on computerised systems and electronic data in 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**.

Annex 2 – Computerised system validation

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

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

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

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**.

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**.

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

The responsible party may also have to **perform additional validation activities** based on a documented assessment or their processes. Vendor should make a test environment available that is identical to the production environment.

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

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

Additional Slices at end of Presentation on Annex 2

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.



2024 US CDISC+TMF Interchange | #ClearDataClearImpact

26

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 or provided 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.



2024 US CDISC+TMF Interchange | #ClearDataClearImpact

27

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 does not 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.



2024 US CDISC+TMF Interchange | #ClearDataClearImpact

28

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, reviewing 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 take 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.



2024 US CDISC+TMF Interchange

Annex 2 Computerised systems validation

A2.4 Traceability of requirements

Traceability should be established and maintained between each user requirement and test cases or 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.



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 define 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 of responsible party and may be specific for a clinical system.

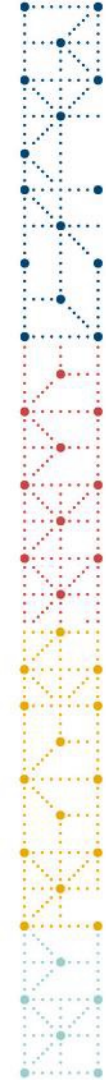
Artifact name	Alternate names	Definition/Purpose
Specification	Requirements	Define the baseline for computer systems validation - what the computer system should do . Common documents for this artifact include (based on scope and magnitude of the computer system): Business/User Requirements , Functional 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 Validation Documentation Release Documentation	<p>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:</p> <p>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</p> <p>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.</p> <p>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)</p> <p>Change Control: The record of system change requests from initial creation through to resolution.</p>

What **might** be included in a **CSV Assurance Process** for a **software as a service** system which passed an audit by the Responsible Party?

- Company's Change Control Process
- Release Notes
- Risk Assessment
 - Evaluated against the previously defined critical functionality
- System's Validation Certificate
- Training, if applicable

If applicable...

- Plan
- Testing Related Records
- Report or similar attestation record



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

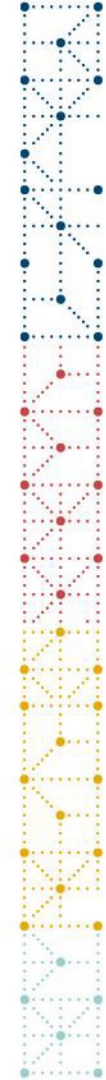


It depends. Not duplicate if the company performed audit of vendor and the vendor passed the audit and the company determined the vendor has adequate process and documentation.

If a software as a service technology is utilized, does this make a difference? Are oversight activities still required to be completed?



Even if SaaS computer system is utilised... and assuming the vendor passed the audit, duplication is not required. However, defining and execution of a Computer System **assurance** process (Risk assessment, Definition of critical functionalities, Plans, Testing, Reports) may be warranted based on many factors.



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



If the system holds TMF records, then the system (a TMF repository) needs to be validated, and oversight process established and performed.

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



System Level: Company repository such as QMS, Trackwise, etc.
Study-specific system or configurations: TMF records so in a TMF repository such as eTMF system.

Are CSA related activities worth it or a waste of time because the technical vendor already tested the system?



Worth it. Considerations...

- 1) Does responsible party have other oversight processes for the technical vendor in place? **Oversight is a responsibility of the sponsor.**
- 2) Audit outcome. There may be identified issues that warrant additional activities by the responsible party.
- 3) Provision of the CSV documentation by technical vendor in a timely manner as EMA directs the responsible party to not use new features until the documentation can be viewed. **This likely impossible if responsible party has purchased the use of the system as a software as a service and are on multi-tenant server.**
- 4) Provision of the CSV documentation at a cost to customers therefore a review of the records is not possible if not purchased.
- 5) Approach to roll out of auto-on features and functionalities. These may not even be used in responsible party's business process. Responsible parties need to define their critical functionalities for a system and oversee any changes.

“I” have contracted a Service Provider who is using a clinical system that is used in my clinical study. Who does the oversight?



REMEMBER: EMA states that: 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 [and processes]*** as adequate.

** Text not in guidance language.*

Service Provider Management of (the Technical Vendor and their) Software used in a Clinical Study:

All oversight begins with:

- 1) Audits **before** any use of the system. Includes CSV process and resultant records. Ensure that critical functionalities are defined in audit scope.
- 2) Defined process to outline oversight and any assurance related activities both at system and study-specific levels that may be required depending on outcome of the audit.

Responsible Party's audit of the Service Provider ensuring processes for oversight may include:

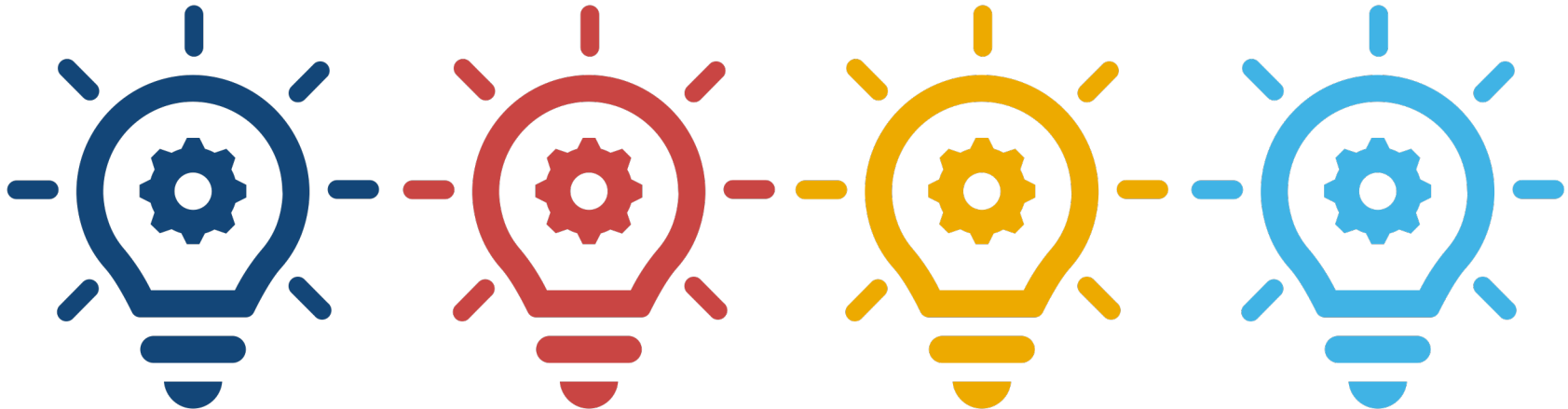
- 1) If Service Provider **is the** technical vendor, audit include CSV processes and resultant records
- 2) If Service Provider's is not technical vendor, the oversight and assurance processes for both system and study-specific configurations

Depending on outcome of the audit, sponsor may need to address Service Provider deficiencies in CSV or technical vendor oversight or take their own actions for attaining assurance, according to their processes.

How will CSV/CSA Records be Included in TMF RM V4?

- TMF Repositories
- Validated
- TMF RM CSV Artifacts
- Oversight and Assurance
- **TMF RM V4**

The TMF RM V4 team has assembled a working group to tackle this question. CSV/CSA related records for the **computerised systems used in clinical studies will be included** in V4 of the TMF RM. Stay tuned!!



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 2025 CDISC+TMF EU Interchange Planning Committee for all the support that they provided me to allow 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 or CSA related documentation/records is a worthwhile effort?



Back-up slides

The CDISC Trial Master File Reference Model – Computer System Validation Tab

Rationale

- The variety of clinical 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."

4.3.4 Validation

- (a) The responsible party is responsible for the validation status of the system throughout its life cycle. The approach to validation of computerised systems should be based on a risk assessment that considers the intended use of the system; the purpose and importance of the data/record that are collected/generated, maintained and retained in the system; and the potential of the system to affect the well-being, rights and safety of trial participants and the reliability of trial results.
- (b) Validation should demonstrate that the system conforms to the established requirements for completeness, accuracy and reliability and that its performance is consistent with its intended purpose.
- (c) Systems should be appropriately validated prior to use. Subsequent changes to the system should be validated based on risk and should consider both previously collected and new data in line with change control procedures.
- (d) Periodic review may be appropriate to ensure that computerised systems remain in a validated state throughout the life cycle of the system.
- (e) Both standard system functionality and protocol-specific configurations and customisations, including automated data entry checks and calculations, should be validated. Interfaces between systems should also be defined and validated. Different degrees of validation may be needed for bespoke systems, systems designed to be configured or systems where no alterations are needed.
- (f) Where relevant, validation procedures (until decommissioning) should cover the following: system design, system requirement, functionality testing,
- (g) The responsible party should ensure that the computerised systems are validated as fit for purpose for use in the trial, including those developed by other parties. They should ensure that validation documentation is maintained and retained.
- (h) Validation should generally include defining the requirements and specifications for the system and their testing, along with the associated documentation, to ensure the system is fit for purpose for use in the trial, especially for critical functionality, such as randomisation, dosing and dose titrations and reductions, and collection of endpoint data.
- (i) Unresolved issues, if any, should be justified and, where relevant, the risks identified from such issues should be addressed by mitigation strategies prior to and/or during the continued use of the system.

The Trial Master File Reference Model – Computer System Validation 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 was 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 Learning Management Systems are not study-specific thus LMS computer systems validation documentation would not be expected to be in scope).



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

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 chooses 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 responsible 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 prior to initial use.

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.