Global Regulatory requirements for Good Manufacturing and Distribution practices in Pharmaceutical /Biopharma industries
COMPUTER SYSTEM VALIDATION (CSV) REQUIREMENTS

Sr. No.	Requirement	Regulatory Reference	Details
VALIDATION DOCUMENTATION & PRACTICES			
1	Inventory List	EU Annex, Pt. 4.3 PIC/s PI-041-1, Section 9.3, Point No. 2.	• Inventory list should be available and it should be a controlled document.
2	Validation Plan User Requirement Specifications	EU Annex 11, Pt. 4 US FDA Part 11.10 (a) EU Annex 11, Pt 4.3 EU Annex 11, Pt. 4.4 PIC/s Pl 041-1, Section 9.2	• CS validation requirement should be covered under Site/Corporate Validation Master Plan. • Separate CS VMP should be available at corporate level and or site level. • PCS requirements should be part of URS. Separate URS for PCS requirements can also be prepared.
3	Risk Assessment Plan	EU Annex 11, Pt. 4.4	• Corporate level and/or site level Risk Assessment guidance document should be available. • Functional Risk Assessments should be carried out for all PCS. • Separate GxP Impact Assessment should be carried out for PCS.
4	System Qualification Tests	EU Annex 11, Pt, 4.7 US FDA Part 11.10(a) PIC/s PI 041-1, Section 9.2.	• Separate PCS qualification protocols should be created. • Installation and Operational Tests should be carried out as per requirements. • There should be adequate link between Risk Assessment and Testing. • Preferably, Separate Validation Summary Report and Requirement Traceability Matrix should be available for PCS.
LIFE CYCLE MANAGEMENT SOPS			

5	System Inventory Management	EU Annex 11, Pt. 4.3	• Inventory should be available & should be governed by respective SOP. • Any addition/deletion/update should be based on this SOP. • Inventory list should also list GMP functionality, validation status, system and process owner for each system.
6	Vendor Assessment	EU Annex 11, Pt. 3 PICs PI-041, Section 10.1, 10.2, 10.3	• To create Vendor Assessment procedure. For all critical systems, vendor assessment to be carried out. • Service Level agreements should be carried out for operational lifecycle support for critical systems
7	Security Management	EU Annex 11, Pt. 12 US FDA Part 11 Pt. 11.10 PICs PI-041.1, Section 9.5	• Common Security policy should be In place for securing OS and Applicant ion usage for authorized use by users to have consistent practices across the company. This should also include password policies and user management, policies of assigning roles and privileges.
8	Incident Management	EU Annex 11, Pt. 13 PICs PI-041, Section 12.1.1.1	• Separate Software Incident Management SOP Is recommended to handle PCS related problems during lifecycle.
9	Data Backup and Restore (also archiving and retrieval)	EU Annex 11, Pt. 7.2, US FDA Part 11.10 (b), (c), (e) PICs PI 041.1, Section 9.9	• SOP for data backup should be available including restore verification frequency. • Data archival and retention SOP should be created. Retrieval process to be defined.
10	Audit Trail Review/ Management (Electronic Data Management)	EU Annex 11, Pt. 9, US FDA Part 11.10 (e), (g)	• Audit trail review/management policy should be available. • Audit trail review SOP should be available for each type of system.

		PICs PI 041.1, Section 9.6	
11	Alarm Review/ Management	US FDA General Principles of Software Validation	• Alarm management policy to be prepared to categorize alarms and review process.
12	Periodic Review	EU Annex 11, Pt. 11, US FDA Part 11.300(e) PICs PI 041.1, Section 9.3 Pt. 5	• Corporate level periodic review Policy/SOP should be created for reviewing validation status of each critical system at predefined frequency. • This review should provide decision for revalidation, if required. Frequency based revalidation should be avoided.
13	Disaster and Recovery Management	EU Annex 11, Pt. 16 Part 11.10(b), (c), (e) PICs PI 041.1, Section 9.9	• Disaster Management SOP should be available for all systems generating electronic data.
14	Remote Access Management	EU Annex 11, Pt. 3.1 PICs PI 041.1, Section 9.3	• Any remote access to vendors should be governed based on Remote Access Management SOP and manual checks to be put in place to verify any impact on any changes carried out by vendor. • Any pre-configured and common ids provided by vendors should be removed or blocked during regular operations.
15	System Retirement SOP	PICs PI 011-3	• System Retirement should be handled through a procedure. The procedure should specify - Data Migration/Archiving - GxP records to be maintained and list of records destroyed - Accessibility and Retrieval of retired Application and Data

Electronic Data Management Verification			
Access Control			
1	Restriction on unauthorized user access to creation, changes and deletion of data. a. Individual Login and password. b. Assignment of roles and privileges for restricted operations. c. User levels and privileges should be documented into SOP	EU Annex 11, Pt. 12 Us FDA Part 11.10 (c), (d), (g), 11.300 (d) PICS Pl 041-1, Section 9.6	• Unique ID & password should be available. OS access control should be based on common IT SOP and configuration should be checked during qualification to demonstrate OS access restriction. • Roles and privileges should be configured in application software. Un-authorized operations should be restricted. Only the Administrator should have access for user management and date/time change. Windows OS access and date/time access should be restricted to Administrator only. All common and vendor provided ids to be either removed or blocked. • SOP for user management should be available. Privileges assignments should be part of machine operation SOP. Remote access through software such as 'Team Viewer' should be available to vendor. The operation during remote access should be monitored. Remote access to vendor should be governed through SOP. Actions by vendors during such access should be monitored and any changes should be noted, through change management procedure.

Audit Trail			
2	Availability and configuration of automatic system generated time stamped audit trail.	EU Annex 11, Pt. 9 US FDA Part 11.10 (e) PICS Pl 041-1, Section 9.6	• Policy should be in place for common expectation of audit trail features and they should be verified during validation.
Data Storage and Backup			
3	Original and Complete Data Storage Backup of data and audit trails Protection and access control to backed up data	EU Annex 11, Pt. 7 US FDA Part 11.10 (c) PICS Pl 041-1, Section 9.9	• Data back-up SOP should be in place. Data storage should be available. Stored data should be backed up as defined in the SOP. Alarms backup should be taken.

GAP ASSESSMENT FOR PCS		
SR. No.	**Check Point**	**Expected Results**
Application Software Checks		
Validation Documentation		
1	Is there any Validation Plan available for the CS Validation?	Validation Plan should be available for CS Validation.
2	Is the System User Requirement Specifications available?	Detailed Document should be available for critical system covering relevant information
3	Has Impact assessment/GxP assessment carried out for the system?	Initial impact assessment based on defined criteria for determining system's validation need should be available. (If GAMPS categorisation is used; classification assessment should be available for the same).
4	Is the System Functional Requirement Specifications available?	Detailed functional specifications from vendor, should be available traceable to URS.

5	Is the Functional Risk Analysis carried out?	Risk Management covering implementation and verification of suitable controls and its observance thereof.
6	Is the System qualification document available?	Computerized System qualification documents IQ/ OQ / PQ should be available.
7	Is overall System Operation using CS verified?	Test should.be available to demonstrate Intended System Operation based on Operation SOP with operation cycle or report printout.
8	Are test evidences available for critical tests?	Evidences by way of either printouts, screenshots or any other approved methods should be available for critical challenge tests.
9	Is Validation Summary Report available?	Summary of validation activities should be documented in Validation Summary Report including any deviations, pending actions and reasons for system acceptance.
10	Is Requirement Traceability Matrix available?	Traceability/matrix linking critical URS to tests should be established for critical systems to demonstrate system acceptance.
Technical Documentation		
1	Are the System Operation and Maintenance Manual available?	Document should be available covering following information- • Detail description for operation process scenario • Instruction to support/removal of the different fault/abnormal condition • Schedule of the regular preventive maintenance task.
2	Is the System configuration record (recipe / set parameters / master record) readily available?	System configuration record should be readily available for review.
3	Is there active technical support from a supplier or principal company available?	Document should be available covering following information-: • Name and contact person name of contractor

		• Duration of Contract • Plan of preventive maintenance schedule visit • SCOPE of the work OR • In case of in house maintenance support, maintenance plan and responsibility
4	Are PLC Input/ Output List available?	Document should be available covering following information – • Service Description of the Input/ Output • IO Address/ Memory Address/ Tag Name
5	Is PLC Bill of Material available?	Document should be available cover following information: • Description of the system Component • Model No. • No. of Qty, • Name of manufacture
6	Is the System Architecture Diagram available?	Document should be available covering following Information: • Connectivity Layout of the different PLC system Components • Connectivity between PLC System-and other devices
7	Is the PLC System Set parameters list available?	Document should be available covering following Information: • All the system Set parameter are noted with its description • Unit Of Measure for the Set Parameter
8	Is the PLC System Process Alarm List available?	Document should be available covering following Information: • All the system Alarm is noted with its description • Alarm Trigger condition

9	Are the PLC System Safety/Process interlock details available?	Document should be available covering following Information: • Interlock Condition/ Scenario • On the Event of Interlock condition system response. • Process sequence • Loop and Logic details
10	Are the Panel Wiring &.As Built Drawings available?	Document should be available covering following Information: • Panel component Layout Drawing with component Identification tag. • Panel wiring details with necessary ferrule Information
11	Is the necessary Spare Requirements list available?	Document should be available covering following Information: • Recommended Spare list from manufacturer with its Item Name • Required Spare Qty • Item Code/ Identification Code
12	Are there Backup copies of software available at site? Is any Development Software available? Can the System Programmer Modification/ Upgrade be done In house?	Backups should be available for all installed software: • PLC program • HMI Program • SCADA application OR Written confirmation from vendor for Willingness to disclose the Loop & Logic configured for the software for an inspection at his site Information from the vendor about its storage location, details of the configured programme files with size.
System Installation		

1	Is the installation of hardware & software available, verified and documented against manufacturer's recommendation? Are these records available?	The hardware/software installation should be verified against manufacturer's recommendation. Records should be available covering following information: • Make/ Manufacturer's name • Model No./Quantity • Basic specification • Location of installation
2	Is the Test Report of the environmental condition available?	Environment condition test report should be available covering following test information: • Actual room environment condition at the time of execution • Record verification of regular monitoring of environment conditions
3	Has the Power and Utility requirement of the PLC verified and documented?	Test report should be available covering following information: • Rating of power circuit protection • Actual reading of power utility at the time of execution
4	Has the PLC panel earthing been verified and documented?	• Earthing of the PLC panel should be proper. • Earthing Drawing should be available.
5	Has the PLC processor & modules arrangement been verified?	PLC processor & modules should be arranged as per System Schematic Drawing.
6	Has the panel component installation and internal wiring arrangement been verified and documented?	Verification report should be available covering following information: • Panel cleanliness • Separation of Higher Voltage and Signal Cable • Existence/ non-existence of unterminated wires
7	Are the Operators and Engineers Trained on PLC System Operation and Maintenance? Are the training records available?	Report should be available covering following verified information: • Training record for authorized personnel with its evaluation procedure

System Operation		
1	PLC Input/ Output functional verification test report.	PLC Input/output functional verification test should be available.
2	Test report of process status in event of power failure & re-establishment of power	Event test report should be available covering following information: • Process status in the event of power failure, • Process status in the event of power re-establishment • Status of set parameters and accumulated values in the event of power re-establishment
3	Test report of different user level security	Test report should be available covering access verification at different level of users.
4	Verification of the set parameter min/max Value Limit (boundary conditions) test report.	Set parameter min/max value limit should be tested and its report should be available.
5	Verification report of the PLC system Diagnostic Alarms	Verification on PLC system Diagnostics alarms status should be available.
6	Test report of equipment status in event of power and communication failure & reestablishment of communication between PLC & HMI/SCADA	Event test report should be available covering following information: • Process status in the event of communication failure. • Process status in the event of power and communication re-establishment. • Status of set parameters and accumulated values in the event of communication re-establishment
7	HMI/SCADA display parameters/ Function Key verification report with actual system operation condition	Display parameter/Function Key should be tested and its result record should be available.
8	Process Alarms with reset response verification report.	Process Alarms should be tested and its result record should be available.

9	Verification of critical interlocks test report.	Interlock should be tested and its result record should be available.
10	Verification of Batch Report printout	Batch report printouts should be taken at end of Individual batch. The report should mention user name, set v/s process parameters, start-end times, changes.
11	Verification of audit trail/event logs Generation	Generation of audit trails for different conditions should be tested as per rights assigned.
Electronic Data Management & Security (21 CFR Part 11)		
Software Access Control and Data Security		
1	Does the system/ software enforce user to enter a password on software start up?	Software should ask a password at the time of software start up.
2	Does the system/ software enforce the user to enter password with specified minimum characters (e.g. 8-10)?	Password length should not be less than predefined characters.
3	Does the system/software allow the creating duplicate username and password combination?	Username and password should be unique. Duplicate username should not be allowed.
4	Does the system/ software has the facility to change password?	Facility for password change should be provided.
5	Does the system/ software has an auto expiry password facility?	Auto password expiry facility should be available and configured.
6	Does the system/software lockout the user account in case of predefined unsuccessful attempts?	Account should lockout after predefined consecutive unsuccessful attempts.
7	Is the application software configured with different levels of user, role and rights?	Application software should be configured for different user levels and its rights.

8	Does only the administrator only has the rights to activate/ deactivate user account?	System administrator only should able to activate or deactivate user accounts
9	Is a user list available for operating system and application software with their assigned roles and rights?	A user list with assigned roles and rights for operating system and application software should be available.
Electronic Audit Trail		
1	Is a date and time stamped audit trail available for all operator/supervisor/admin entries and actions?	A date and time stamped audit trail should be available for all operator entries and actions.
2	Is the audit trail log record protected and stored safely?	Audit trail log record should not be accessed by normal user and stored at secured location.
3	Is the database of logged data encrypted?	Database of logged data should be encrypted.
4	Is the transaction type (inserts/delete/modify) associated with the transaction in audit trail?	Audit trail should mention the type of transaction.
5	Is previous data/record available?	Record changes shall not obscure previously recorded information. New value and old Value after record changes are captured.
6	Is audit trail backed up?	Audit trails should be backed up and retained as per retention policy.
Data Backup		
1	Is data back and restore based on SOP?	SOP should be available for Data backup and Restore.
2	Are the electronic record archived in the system?	If the electronic records arc available in the system, then old data backup should be available at backup location. The URS/FS of system should reflect e-records and backup management requirement.

3	Does the system have the facility to Store, backup and restore backup data?	Data Storage, Backup and restore data from backup device should be available.
4	Is the data backup and restore facility authorised to system administrator only?	Provision for data backup and restore should restricted to authorised persons only.
5	Is the data record available up to retention period?	Backup record should be maintained for the retention period policy and the same should be defined.
6	Is there a reliable data storage media selected for data backup?	Backup data should be stored on removable media/ tape drives. Backup media quality test certificate should be available.
7	Is there a procedure available for the identification of data backup media?	There should be more than one Backup media (In quantity) and they are used on rotational basis.
8	Is the backup available on more than one media and backup frequency ls defined?	There should be more than one Backup media (In quantity) and they are used on rotational basis.
9	Is the data backup media stored at safe place?	Backup data should be stored in safe and secured place.
10	Is the redundant data backup device available?	Spare backup device should be available.
11	Is training record available for persons handling data backup and restore?,	Training record with evaluation form should be available for the person/s that arc responsible for backup and restore of the data.
12	Is a 1ist of files/folders clearly identified from which the backup is taken / to be taken?	Flies/folders should be clearly identified as to which backup ls taken/ to be taken.
13	Is there a procedure to handle Disaster Recovery?	SOP should be In place. Data backup logs should be available. Periodic restoration Is verification carried out.

14	Are backed up data verified periodically?	Data backup logs should be available. Periodic restoration & its verification is carried out.
Electronic Signature		
1	Does signed electronic record contain information associated with the signing?	Signed electronic records contain information associated with the signing that clearly indicates all of the following: 1. The printed name of the signer (full name). 2. The date and time (time for electronic signature only when the signature was executed. 3. The meaning of the signing (such as approval, review, responsibility, or authorship) associated with the signature.
2	Are Electronic Signatures linked to their electronic records?	Electronic Signatures are linked to their electronic records and ensure that e-sign cannot be excised, copied or transferred.
3	Are Electronic Signatures Unique?	Electronic signatures are unique to an individual and cannot be reused by, or reassigned to anyone else. Identity of an Individual verified before an electronic signature is allocated.
Operating System Checks		
1	Is User Unable to access the Desktop without separate user ID to login to OS?	Separate user Id an password should be assigned to user for logging into OS.
2	Does the OS enforce user to enter a password on system power up?	Power-on passwords should be implemented on the OS.
3	Does the OS access automatically lock in when left unattended?	Screen savers with automated time out should be installed on all workstations.
4	Does the OS enforce user to enter specified characters password?	Password length should not be less than specified characters.

5	Does the OS allow creating duplicate username and password combination?	Username and password should be very unique.
6	Does the system has facility to change password?	Facility for password change should be provided.
7	Does the system has an auto expiry as password facility?	Auto password expiry facility should be available and configured.
8	Does the OS lockout the user account in case of Identified unsuccessful attempts?	Account should lockout after predefined consecutive unsuccessful attempts. Unlock should be through system admin.
9	Has the OS been configured with different levels of user, role and right?	System should be configured with different user levels and Its rights.
10	Does the administrator alone has the rights to activate/deactivate user accounts?	System administrator only should able to active or deactivate user accounts.
11	Is the desktop date and time secured and synchronized with server date and time?	Only administrator can set the desktop date and time. A desktop on the network should have the date and time synchronized with server date and time.
12	Has the time zone of system is set as applicable and cannot be changed by any user?	System date, time and time zone shall not be accessed *to* user and can be accessed by administrator only.
13	Is the logged data folder secure and only administrator can access it?	Logged data folder file should be secured and only system administrator should have logged data file access rights.
14	Is the system on the network? If yes, any data shared for remote access? If yes, is the security for the shared data implemented?	The shared data of the OS should be secured.
15	Does the OS generate a log record for following? All log on attempts	Log record of all log attempts and use of user accounts with OS should be available.

	Use of user accounts with system	
16	Is anti-virus software Installed on the system?	Antivirus software should be installed on the OS.
17	Is anti-virus software updated regularly?	The installed antivirus software should be updated regularly.
18	Is compatibility of software is assessed with antivirus for application software?	System validation should provide compatibility.
19	Is cut/ copy /paste/ replace rights are disabled?	For user cut/copy/paste/replace rights should not be allowed.
20	Is right click option/ task bar option disabled?	Right click option should be disallowed for users.
21	Is USB/CD access to system restricted?	System should not have USB /CD drive available for users
22	Is system folder access restricted?	OS folder access should not be allowed to user. Data copy/paste option should not be available. Control panel; command prompt access should not be allowed to users.
23	Is recycle bin restricted for user? .	Recycle bin should be restricted to user.
24	Is USB drive active and can be accessed by user?	USB drive, CD drive access of use should be restricted for user and can only be accessed by administrator.
25	Are there office productivity software installed and can be accessed by user?	User should not have any access to office productivity tools such as MSWORD, EXCEL, Paint, Notepad.
26	Is File Access through Start.exe (If applicable) is available for user?	File Access Restriction through Start.exe (If applicable) to be available for user.

References

1. EU Volume 4 - Good Manufacturing Practice Medicinal Products for Human and Veterinary Use, Annex 11: Computerised Systems (SANCO/C8/AM/sl/ares(2010)1064599) dated June 2011
2. EDQM - Validation Of Computerised Systems - Core document (PA/PH/OMCL (08) 69 R7) dated August 2018
3. PIC/S Guidance. Good Practices For Data Management And Integrity In Regulated GMP/GDP Environment. PI-041-1. July 2021
4. PIC/S Guidance. Good Practices for Computerised Systems in Regulated "GXP" Environments - PI 011-3. September 2007
5. US FDA 21 CFR Part 11 Electronic Records; Electronic Signatures. (up to date as of 9/19/2024)
6. US FDA General Principles of Software Validation; Final Guidance for Industry and FDA Staff Document issued on: January 11, 2002

Additional References

1. ICH Harmonised Tripartite Guideline, Good Manufacturing Practice Guide for Active Pharmaceutical Ingredients. **Q7.** Current Step 4 version dated 10 November 2000
2. GAMP 5 – A risk based approach to compliant Gxp computerised systems.
3. EMA - Notice to sponsors on validation and qualification of computerized systems used in clinical trials. (EMA/INS/GCP/467532/201907) April 2020
4. EDQM - Validation Of Computerized Systems - Core document (PA/PH/OMCL (08) 69 R7) dated August 2018
5. Canada - Annex 11 to the good manufacturing practices guide: Computerized Systems: GUI-0050 dated August 2021
6. US FDA Guidance for Industry - Computerized Systems Used in Clinical Investigations dated May 2007
7. US FDA Guidance for Industry - Computerized Systems Used In Clinical Trials dated April 1999
8. WHO Guidelines on Validation – Appendix 5 - Validation of Computerized Systems (Draft guideline dated August 2018)
9. WHO Annex 3 - Good manufacturing practices: guidelines on validation - WHO Technical Report Series, No. 1019, 2019

Few Abbreviation's

- PCS -Personal Communications Service
- SOP-Standard Operating Procedure
- OS- Operating System
- CS-Computerized System
- VMP-Validation Master Plan
- URS – User Requirements System
- ID- Identification
- IT -Information Technology

ASSESSMENT FOR CSV