ChatGPT

Computer System Validation for AI Software

1. CSV Fundamentals

Computer System Validation (CSV) is a structured process to ensure that computerized systems used in pharmaceutical operations perform reliably and meet predefined requirements [1]. CSV matters because patient safety, product quality and data integrity increasingly depend on software-controlled systems. Validated systems produce accurate and consistent data, helping to prevent errors that could harm patients or compromise product quality [1]. The traditional CSV lifecycle follows a V-model: starting with planning and user requirements, progressing through design, installation (IQ), operational (OQ) and performance qualifications (PQ), and culminating in a validation report and ongoing maintenance [2] [3]. Risk-based CSV aligns with GxP risk management: critical systems (e.g. batch records, QC software) receive rigorous testing, while lower-impact systems get a lighter touch. GAMP 5 guidance embodies this philosophy, categorizing systems by complexity and customizing validation accordingly [4].

2. Traditional CSV Documentation

Key deliverables in CSV include: - **Validation Master Plan:** Defines scope, roles, and approach for all validation activities. - **User Requirements Specification (URS) / Functional Requirements (FRS) / Design Specifications (DS):** Documents what the system must do (URS/FRS) and how it is implemented (DS). These trace to tests. - **Risk Assessment:** Evaluates how failures could impact quality/patients and determines the validation rigor needed. - **Test Protocols (IQ, OQ, PQ):** Step-by-step test plans and acceptance criteria for installation, functionality and performance tests. - **Traceability Matrix:** A table linking each requirement to one or more test cases, ensuring full coverage. - **Validation Report:** Summarizes all validation activities, test results, deviations and final conclusions about the system's fitness. - **SOPs and Training:** Operating procedures for the system and documented training of users and operators.

These documents provide the evidence that the system was built and tested according to GxP standards, with all deviations handled.

3. How AI Complicates CSV

AI-based software challenges these norms in several ways: - **Variable, Non-Deterministic Outputs:** Unlike fixed logic software, AI (especially machine learning models) can produce different results on the same input, especially if there are elements of randomness. This makes it impossible to define a single "expected result" ahead of time for every test. - **Learning Models:** Models that are retrained or continuously updated during use can change behavior post-deployment. Traditional validation assumes the code under test is static; AI models may adapt over time, invalidating earlier test evidence. - **Vendor Opacity:** Many AI tools (particularly cloud AI services) are proprietary "black boxes." The user may not know exactly how the model works internally, which conflicts with the transparency needed for CSV. - **Impossible to Predefine All Outputs:** For something like a language model or recommendation engine, the range of possible outputs is enormous. We cannot write test cases for every possible input. This breaks the conventional IQ/OQ/PQ

testing approach. - **Need for Review Strategies:** Because we cannot predict AI outputs, validation often requires human review of AI-generated content. For example, testing an AI that summarizes documents might involve sampling outputs and checking quality, rather than hard-coded expected values. - **Impact of Model Updates:** If a vendor updates the underlying model or retrains it, the system's behavior may change without any change to our code. This means we must control model versions (e.g. pin to a fixed model) and treat updates like change control events. In sum, AI's unpredictable and evolving nature means traditional CSV must be adapted. We often validate AI components by statistical testing, monitoring and governance rather than deterministic test cases.

4. Risk-Based Application

The extent of CSV needed for an AI feature depends on its intended use (risk level):

- **Low-Risk Uses:** Examples are *drafting support* or *summarization tools* (e.g. an AI that suggests text for SOPs or literature summaries). Since humans review and approve all outputs, the CSV can be minimal. Key steps are supplier qualification, accuracy checks on typical cases, and guidance on proper use.
- **Medium-Risk Uses:** Tools like *search/retrieval* or *data classification* that aid analysts or highlight possible items. These affect efficiency but do not directly make quality decisions. They require validation of accuracy (e.g. relevant results retrieved) and controls to ensure operators verify the AI's suggestions.
- **High-Risk Uses:** Functions like *anomaly detection* in manufacturing data or *decision support* for quality release. These could directly influence product quality if wrong. They need rigorous validation: well-defined performance metrics, extensive testing on historical data, and documented limits of operation. Human oversight is mandatory – the AI should assist, not replace, expert judgment.
- **Critical Uses:** Fully automated decision-making (e.g. an AI that autonomously sets process parameters or batch approval) would be extremely high risk. Such uses would essentially need to be validated as formal processes themselves, possibly requiring regulatory review.

Regulators expect the validation effort to match risk. For example, an AI "smart filter" for CAPA triage (medium risk) may have a simpler plan than an AI that predicts batch failure in real-time (high risk). This risk-based approach is aligned with existing CSV practices.

5. Governance Model

To manage AI tools, QA/CSV teams should extend their governance to cover:

- **Access Controls:** Restrict who can use the AI feature and in what mode. For instance, disable "self-training" features for end users to prevent untracked model updates.
- **Procedural Restrictions:** Define approved use cases explicitly. Users should follow SOPs on when/how to run the AI, how to interpret results, and how to document its use in controlled records.
- **Review Requirements:** Mandate that any output impacting quality decisions be reviewed and signed off by qualified personnel. Consider implementing a two-person rule for high-impact AI outputs.

- **Periodic Performance Review:** Similar to equipment calibration, periodically assess the AI's performance on representative data. For example, track accuracy or false alarm rates over time. If performance degrades, investigate and retrain or revert model.
- **Change Control:** Any modification to the AI (software updates, retraining, configuration changes) must go through formal change control. This includes changes by the vendor.
- **Model Documentation and Traceability:** Maintain records of model versions, training data snapshots, and any tuning parameters. This mirrors version control and provides traceability for audits.

In practice, an AI governance framework involves QA, IT, and data science teams. For example, one might create an "AI Quality Board" that reviews new AI tools, classifies risk, and oversees validation strategy. This cross-functional oversight is crucial given AI's novelty in GxP contexts [4].

6. Top 3 AI Tools/Platforms for CSV-Controlled Use

The following AI platforms are noted for their enterprise focus and governance features, making them more amenable to CSV:

Platform	Use Case	Strengths	Weaknesses	CSV Relevance	Governance Advantages
Microsoft Azure AI (OpenAI Service)	Controlled generative AI (e.g. document drafting, Q&A)	Enterprise compliance (ISO/SOC/HIPAA). Azure offers role-based access, auditing, and ability to deploy models in a virtual network. Supports "OpenAI function calling" and filters for safety.	Large language models can hallucinate; requires careful prompt management. Vendor controls model updates (need fixed deployments). Mostly cloud-based.	High – Azure provides infrastructure for 21 CFR 11 compliance (audit trails, encrypted logs). Validation focuses on access and data controls rather than model internals.	Strong identity/role management, logging of all API calls, Azure Policy for content filtering, ability to use private endpoints.

Platform	Use Case	Strengths	Weaknesses	CSV Relevance	Governance Advantages
IBM Watsonx (Data & AI)	AI analytics and text processing	Offers tools for model interpretability (AI Explainability 360), data lineage and governance. Can be hosted on-prem or private cloud.	Complex suite – steep learning curve. Native focus on models (not an LLM chat service).	High – Designed for regulated data analytics. Built-in audit logging and model documentation help CSV.	Comprehensive governance (IBM OpenPages), integrated AI FactSheets, and automated reporting of model metrics.
DataRobot Enterprise MLOps	Predictive modeling and automated compliance docs	Auto-generates documentation for model training and performance. Tracks data lineage, versioning and provides model explainability (feature impact). Low-code interface speeds development.	Primarily suited for structured data models, not generative AI. Cloud or on-prem options needed.	High – Tailored to regulated industries. Focuses on documenting everything needed for validation (data, code, results).	Built-in risk assessment templates, audit trails of model changes, governance dashboard with user access controls.

- **Microsoft Azure AI (OpenAI Service):** Suited for AI features in business apps (e.g. summarizing batch records). Its enterprise-grade platform supports CSV via network isolation, authentication, encryption and logging. However, LLM outputs must be carefully controlled, so CSV will emphasize stringent user training and output review.
- **IBM Watsonx:** Best for AI data pipelines and language tasks. Watsonx's emphasis on explainability and modular deployment (cloud or on-prem) aligns well with validation. QA can leverage its fact-sheet generation to understand model behavior. Its complexity may require more technical effort.
- **DataRobot MLOps:** Excels at building and deploying predictive models (e.g. CAPA recurrence risk). It automatically creates an "audit trail" of data prep and model decisions, which greatly aids validation. It's less applicable for LLM tasks but strong for algorithmic AI in QMS.

Each platform can enforce policies (Azure Active Directory, IBM identity, DataRobot roles) and produce audit logs of AI use – key for CSV documentation. They differ in specialization: Azure OpenAI is generative, Watsonx is a broad AI suite, and DataRobot focuses on machine learning workflows. All support enterprise security features that CSV demands.

7. Final Guidance

When assessing an AI-enabled tool under CSV:

- **Classify the risk:** Determine how the AI output affects patient safety or quality. Low-risk tools need lighter CSV (focusing on data integrity), while high-risk tools require full validation.
- **Validate like a system:** Adapt CSV V-model steps to AI. Define requirements (even if vague, e.g. “assist, not decide”), plan tests (or review strategies), document architecture, and create clear acceptance criteria (e.g. “95% of classifications match historical labels”).
- **Emphasize data and oversight:** Ensure training data and input sources are validated. Establish procedures for human review of AI output. Document how a user should verify or override the AI.
- **Control changes:** Lock down the AI model version in production. Any update must pass a mini-validation. If using a vendor-hosted AI, contractually require notification of model changes.
- **Monitor continuously:** Set up performance metrics and dashboards for the AI (e.g. error rates). If drift is detected, investigate and, if needed, retire or retrain the model under a change control protocol.
- **Maintain documentation:** Keep all model-related documentation (model files, training logs, performance reports) under version control. This aids inspections and audits.

In essence, treat the AI tool as a computerized system subject to 21 CFR 11 and GMP controls. Leverage the built-in governance of enterprise AI platforms, and build a CSV strategy around intended use and risk. With careful planning, training of users, and robust oversight, AI features can be incorporated without compromising compliance. The key is balancing innovation with the discipline of validation: let AI speed up tasks but hold every result to the same standards of reliability required in pharma.

Sources: Key references included peer-reviewed reviews on CSV and AI in pharma [1] [4] and vendor literature on platform governance [1] [4]. These informed the guidance on adapting CSV principles to AI-enabled systems.

---

[1] [2] [3] The Essential Guide to Computer System Validation in the Pharmaceutical Industry - PMC
https://pmc.ncbi.nlm.nih.gov/articles/PMC11416705/

[4] Regulatory Perspectives for AI/ML Implementation in Pharmaceutical GMP Environments - PMC
https://pmc.ncbi.nlm.nih.gov/articles/PMC12195787/