AI Validation Readiness Assessment

GMP / GxP AI System Validation Readiness Template

Prepared for AIforQA.org

Document No.		**Version**	
Effective Date		**Page**	
AI System / Tool		**Business Process**	
Site / Department		**Assessment Date**	

1. Short Description

This assessment helps QA, CSV, Validation, IT Quality, System Owners, and Business Process Owners determine whether an AI system is ready for formal validation planning before creating a validation plan, User Requirements Specification (URS), risk assessment, or test strategy in a GMP/GxP environment.

2. Intended Use

Use this assessment before or during the planning phase for AI systems that may support, influence, generate, analyze, review, or route GxP data, records, processes, or decisions. This includes:

- AI software implementation within or adjacent to GMP/GxP processes.
- AI functionality integrated with QMS, LMS, LIMS, MES, ERP, document management, deviation, CAPA, complaint, training, or validation systems.
- AI document review, SOP comparison, document classification, or regulated content analysis systems.
- AI analytics tools used for CPV, trend analysis, complaint trending, maintenance prediction, calibration drift, or quality risk monitoring.
- AI-enabled decision support systems used by QA, validation, manufacturing, QC, regulatory, compliance, or IT Quality teams.
- Machine learning model deployment, model retraining, model monitoring, or externally hosted AI services used in a GxP context.

3. Scope

Included	Excluded / Out of Scope
AI systems, AI features, machine learning models, generative AI tools, vendor platforms, internal analytics tools, and AI-enabled workflows that may affect GxP records, regulated processes, quality decisions, compliance decisions, data integrity, or validation state.	Personal productivity tools with no GxP use, informal brainstorming not connected to quality decisions, consumer AI use outside company systems, and fully manual processes with no AI functionality. Exclusion should be justified if the tool is available to GxP personnel.

4. User Instructions

1. Identify the AI system, vendor, version, deployment model, process owner, and intended GxP or non-GxP use.

2. Complete the System Information Table before answering readiness questions.

3. Answer each checklist question as Yes, No, or N/A. Use N/A only when the item truly does not apply and provide justification.

4. For every No answer in a required or high-risk area, document the risk impact and required action before validation planning proceeds.

5. Classify readiness using the scoring criteria in Section 10.

6. Define recommended validation strategy actions in Section 11.

7. Attach or reference supporting evidence, such as vendor documentation, architecture diagrams, data flow diagrams, SOPs, security assessments, and prior risk assessments.

8. Route the completed assessment for QA, CSV/Validation, IT Quality, System Owner, and Business Process Owner review as applicable.

5. Key Definitions

Term	Definition
AI system	Software, platform, application, model, feature, or workflow that uses artificial intelligence, machine learning, natural language processing, generative AI, rules plus AI analytics, or related techniques to generate, classify, analyze, predict, recommend, summarize, or support decisions.
Machine learning model	A computational model that learns patterns from data and produces outputs such as predictions, classifications, rankings, recommendations, summaries, or anomaly flags.
Intended use	The approved and documented purpose for which the AI system will be used, including users, supported process, data inputs, outputs, limitations, and whether outputs may influence GxP decisions.
GxP impact	The potential for the system, data, output, or workflow to affect GMP, GLP, GCP, GDP, regulated records, product quality, patient safety, compliance, validation state, or regulatory commitments.
Validation readiness	The degree to which the system, intended use, requirements, data flows, supplier documentation, risks, and controls are sufficiently defined to begin formal validation planning.
User requirements	Documented business, compliance, functional, technical, security, data integrity, reporting, and performance needs that the validated system must satisfy.
Data input	Data, documents, prompts, records, metadata, interface feeds, sensor data, transaction data, or user-entered information provided to the AI system.
Data output	Any AI-generated result, classification, recommendation, prediction, summary, risk score, report, extracted information, alert, or decision-support output.
Model monitoring	Ongoing review of AI model performance, drift, accuracy, false positives, false negatives, user overrides, data changes, and continued fitness for intended use.
Change control	A documented quality process used to evaluate, approve, implement, and verify changes that may affect validated state, GxP processes, data integrity, security, or compliance.

6. System Information Table

Field	Response	Field	Response
System name		**Vendor**	
Version / release		**System owner**	
Business process owner		**GxP process supported**	
Intended use		**Deployment model**	
Cloud / on-premise		**Interfaces**	
Data sources		**Output types**	
AI / ML functionality summary		**Primary user groups**	
Regulated records impacted		**Proposed go-live / deployment date**	

7. Validation Readiness Checklist

Complete each line item before validation planning is finalized. “No” responses should be evaluated for impact and may require remediation before the system is considered ready.

Area	Question	Yes	No	N/A	Risk Impact	Comments / Evidence
Intended use clarity	Is the intended use clearly defined, documented, and approved by the business process owner and QA/CSV as applicable?	☐	☐	☐		
Intended use clarity	Does the intended use define what the AI system may do and what it is prohibited from doing?	☐	☐	☐		
Intended use clarity	Are users, user groups, supported processes, and decision boundaries clearly identified?	☐	☐	☐		
Intended use clarity	Are limitations, assumptions, and known constraints documented?	☐	☐	☐		
GxP impact	Has a documented GxP impact assessment been performed or planned?	☐	☐	☐		
GxP impact	Could the system affect product quality, patient safety, compliance, batch disposition, validation state, or regulated records?	☐	☐	☐		
GxP impact	Are GxP and non-GxP functions clearly separated where applicable?	☐	☐	☐		
GxP impact	Has the degree of AI influence on GxP decisions been classified?	☐	☐	☐		
User requirements	Are draft user requirements available or sufficiently defined to begin URS development?	☐	☐	☐		
User requirements	Do requirements include functional, compliance, data integrity, security, audit trail, reporting, and model monitoring needs?	☐	☐	☐		
User requirements	Are AI-specific requirements included, such as explainability, source traceability, output review, and model/version control?	☐	☐	☐		
User requirements	Have process owners and SMEs reviewed the proposed requirements?	☐	☐	☐		
Data inputs	Are all data inputs identified, including user prompts, documents, records, interfaces, databases, sensor data, or file uploads?	☐	☐	☐		
Data inputs	Are data sources controlled, approved, current, and appropriate for the intended use?	☐	☐	☐		
Data inputs	Are data input transformations, filtering, normalization, exclusions, or preprocessing steps defined?	☐	☐	☐		
Data inputs	Are restrictions defined for confidential, proprietary, patient, batch, or regulated data entered into the AI system?	☐	☐	☐		
Data outputs	Are all output types identified, such as summaries, classifications, recommendations, predictions, risk scores, alerts, or reports?	☐	☐	☐		
Data outputs	Is it clear whether outputs are advisory, draft, decision-supporting, or decision-executing?	☐	☐	☐		
Data outputs	Are AI outputs traceable to source data, source documents, model version, and user context?	☐	☐	☐		
Data outputs	Are acceptance criteria or review criteria defined for AI outputs?	☐	☐	☐		
Algorithm/model behavior	Is the AI model type or AI function sufficiently understood for validation planning?	☐	☐	☐		
Algorithm/model behavior	Is model explainability or rationale available at a level appropriate for the intended use and risk?	☐	☐	☐		
Algorithm/model behavior	Are known risks such as hallucination, false positives, false negatives, bias, model drift, and overreliance addressed?	☐	☐	☐		
Algorithm/model behavior	Can the model or configuration be version-controlled and locked for validated use where required?	☐	☐	☐		
Audit trail	Does the system generate audit trails for creation, modification, deletion, review, approval, override, and use of regulated records or outputs?	☐	☐	☐		
Audit trail	Can AI recommendations, user actions, accepted/rejected outputs, and final human decisions be reconstructed?	☐	☐	☐		
Audit trail	Are audit trail review expectations defined for GMP-relevant use?	☐	☐	☐		
Electronic records/signatures	Has 21 CFR Part 11 / Annex 11 applicability been assessed or planned?	☐	☐	☐		
Electronic records/signatures	Are electronic signatures, if used, attributable to specific users with date, time, meaning, and record linkage?	☐	☐	☐		
Electronic records/signatures	Are records retained, retrievable, protected, and available for inspection for the required retention period?	☐	☐	☐		
Access control	Are role-based permissions defined for users, administrators, reviewers, approvers, and support personnel?	☐	☐	☐		
Access control	Can unauthorized users be prevented from modifying models, configurations, records, prompts, outputs, or approval workflows?	☐	☐	☐		
Access control	Are user provisioning, deactivation, periodic access review, and privileged access controls	☐	☐	☐		

Area	Question	Yes	No	N/A	Risk Impact	Comments / Evidence
	defined?					
Data integrity	Are ALCOA+ principles addressed for data inputs, outputs, records, review decisions, and retained evidence?	☐	☐	☐		
Data integrity	Are original source data preserved and protected from being overwritten by AI-generated summaries or transformations?	☐	☐	☐		
Data integrity	Are manual data exports, uploads, and integrations controlled and reconciled where required?	☐	☐	☐		
Supplier documentation	Has the vendor provided sufficient documentation for validation planning, including system description, architecture, AI functionality, release notes, security, and support model?	☐	☐	☐		
Supplier documentation	Are supplier qualification, vendor assessment, or supplier audit needs identified?	☐	☐	☐		
Supplier documentation	Are service level agreements, data use terms, subcontractors, data residency, and support responsibilities understood?	☐	☐	☐		
Testing strategy	Can test cases be designed to verify user requirements, workflows, interfaces, security, audit trail, reports, and data integrity?	☐	☐	☐		
Testing strategy	Are AI-specific tests planned, such as known-case testing, edge cases, false positive/negative review, output verification, and performance thresholds?	☐	☐	☐		
Testing strategy	Are IQ/OQ/PQ or equivalent lifecycle testing expectations understood?	☐	☐	☐		
Model monitoring	Is there a defined approach for monitoring model performance after go-live?	☐	☐	☐		
Model monitoring	Are model drift, retraining, configuration changes, data changes, and performance degradation addressed?	☐	☐	☐		
Model monitoring	Are periodic review metrics defined, such as accuracy, rejected outputs, overrides, incidents, user feedback, and missed signals?	☐	☐	☐		
Change control	Are changes to model, prompts, configuration, workflows, interfaces, source data, vendor releases, and deployment environment controlled?	☐	☐	☐		
Change control	Are revalidation or regression testing triggers defined?	☐	☐	☐		
Change control	Is there a process for emergency fixes, rollback, and impact assessment?	☐	☐	☐		
Periodic review	Is a periodic review process defined for continued fitness for intended use?	☐	☐	☐		
Periodic review	Will open issues, deviations, incidents, complaints, audit findings, and performance trends be reviewed periodically?	☐	☐	☐		
Cybersecurity	Has cybersecurity risk been assessed or planned, including authentication, encryption, logging, vulnerability management, and incident response?	☐	☐	☐		
Cybersecurity	Are cloud hosting, data residency, backup, disaster recovery, and business continuity controls understood?	☐	☐	☐		
Cybersecurity	Are AI-specific threats considered, such as prompt injection, data leakage, unauthorized model access, and malicious output manipulation?	☐	☐	☐		

8. Readiness Scoring

Readiness Outcome	Criteria	Required Action
Ready for validation planning	Intended use is clear; GxP impact is understood; core requirements, data flows, outputs, supplier information, system ownership, and validation approach are sufficiently defined; no unresolved critical gaps remain.	Proceed with validation plan, URS, risk assessment, and test strategy.
Conditionally ready	Most readiness elements are defined, but limited gaps remain that can be resolved during early validation planning without delaying risk assessment or URS development.	Proceed with caution; document open items, owners, and due dates before validation execution.
Requires further assessment	Important information is incomplete, such as GxP impact, intended use, data sources, outputs, model behavior, supplier documentation, or Part 11 applicability.	Pause formal validation planning until additional assessment and supporting evidence are available.
Not ready	Critical gaps exist, such as undefined intended use, unknown data sources, uncontrolled GxP impact, no supplier documentation, unclear model behavior, or no feasible validation/testing strategy.	Do not proceed. Escalate to QA/CSV/IT Quality and complete remediation before validation planning.

Selected readiness outcome: ☐ Ready for validation planning ☐ Conditionally ready ☐ Requires further assessment ☐ Not ready

9. Validation Strategy Recommendations

Validation Area	Recommended Planning Considerations
URS	Define business process, GxP intended use, user roles, data inputs, AI outputs, decision boundaries, human review, data integrity, reporting, audit trail, security, and model monitoring requirements.
Risk assessment	Assess impact on product quality, patient safety, regulated records, compliance decisions, batch disposition, validation state, data integrity, and cybersecurity. Include AI-specific risks such as hallucination, drift, false positives/negatives, and overreliance.
IQ/OQ/PQ	Plan installation/configuration verification, functional workflow testing, user requirement testing, role-based access testing, audit trail testing, interface testing, report testing, backup/recovery, and process performance testing as applicable.
Data integrity testing	Verify ALCOA+ controls, source data preservation, output traceability, audit trails, record retention, data migration/import, interface reconciliation, time stamps, and user attribution.
Part 11 assessment	Assess electronic records, electronic signatures, audit trails, access controls, system validation, record retention, authority checks, and availability for inspection.
Supplier audit / qualification	Evaluate vendor quality system, software development lifecycle, release management, AI model documentation, cybersecurity, data privacy, hosting, support, change notification, and validation support documentation.
Model performance monitoring	Define performance metrics, expected accuracy, known-case testing, acceptance thresholds, drift monitoring, exception handling, false positive/negative review, override tracking, and escalation triggers.
Periodic review	Plan periodic review of system performance, incidents, access, audit trails, model/configuration changes, vendor releases, user feedback, deviations, CAPAs, cybersecurity events, and continued fitness for intended use.

10. Required Documentation

Retain or reference the following records as applicable:

- Completed AI Validation Readiness Assessment.
- GxP impact assessment and preliminary risk assessment.
- System description, architecture diagram, and data flow diagram.
- Intended use statement and AI use boundaries.
- Draft or approved URS and requirements traceability matrix.

- Supplier/vendor qualification records and vendor documentation.
- Part 11 / Annex 11 assessment, if applicable.
- Cybersecurity and privacy assessments.
- Validation plan, test strategy, IQ/OQ/PQ protocols, test scripts, and summary report when created.
- Model performance testing and monitoring plan.
- Change control records and release/version documentation.
- Training records for users, reviewers, approvers, administrators, and support personnel.
- Periodic review records after implementation.

11. Approval Table

Role	Name	Department	Signature	Date	Comments
Prepared by					
Reviewed by					
Approved by					
CSV / Validation Review					
IT Quality Review					
System Owner / Business Process Owner					

12. Disclaimer

This tool is intended as a practical quality assurance aid and does not replace company procedures, regulatory requirements, or formal validation/compliance review.

13. Website Integration Block

Field	Recommendation
SEO title	AI Validation Readiness Assessment for GMP and GxP Systems
Meta description	Assess whether an AI system is ready for GMP validation planning, URS, risk assessment, and testing.
Recommended URL slug	/tools/ai-validation-readiness-assessment
Recommended tags	AI validation, CSV, GMP, GxP, Part 11, AI governance, quality systems, data integrity, validation readiness
Short website excerpt	A practical GMP/Pharma QA template to assess whether an AI system is ready for formal validation planning in regulated environments.
Related AIforQA.org article ideas	AI Validation in GMP: What QA and CSV Teams Need to Know; What Happens When AI Makes a GMP Mistake?; AI for GMP Document Review and Approval Workflows; AI for Pharmaceutical Risk Management Under ICH Q9
Suggested internal links	AI Tool GMP Risk Assessment Checklist; ChatGPT / AI Use Log for QA Teams; AI-Generated Content Review Checklist; AI for Batch Record Review by Exception; AI and Pharmaceutical Knowledge Management