Computer System Validation Checklist

From URS to System Release

A practical guide for validation engineers, QA teams, IT quality specialists, system owners, consultants, and pharma learners

- **Risk-based approach**
- **Inspection-ready documentation**
- **Practical release checklist**

How to Use This Guide

Use this deck as a practical roadmap for planning, documenting, reviewing, and releasing a GxP computerized system.

1

1. Define scope

Clarify intended use, users, and boundaries

2

2. Build the package

URS, risk assessment, specs, and plan

3

3. Verify the system

Test, trace requirements, and resolve deviations

4

4. Release and maintain

Approve, train users, and control changes

Best for: QA, IT quality, system owners, consultants, and learners

Tip: Use the final checklist before go-live

What CSV Must Demonstrate

Computer system validation should provide clear evidence that the system is fit for its intended GxP use.

Works as intended

Core functions perform correctly and consistently

Risks are controlled

Critical failures are identified and reduced

Data are reliable

Records are accurate, secure, and complete

Controls are effective

Access, audit trail, and change control are in place

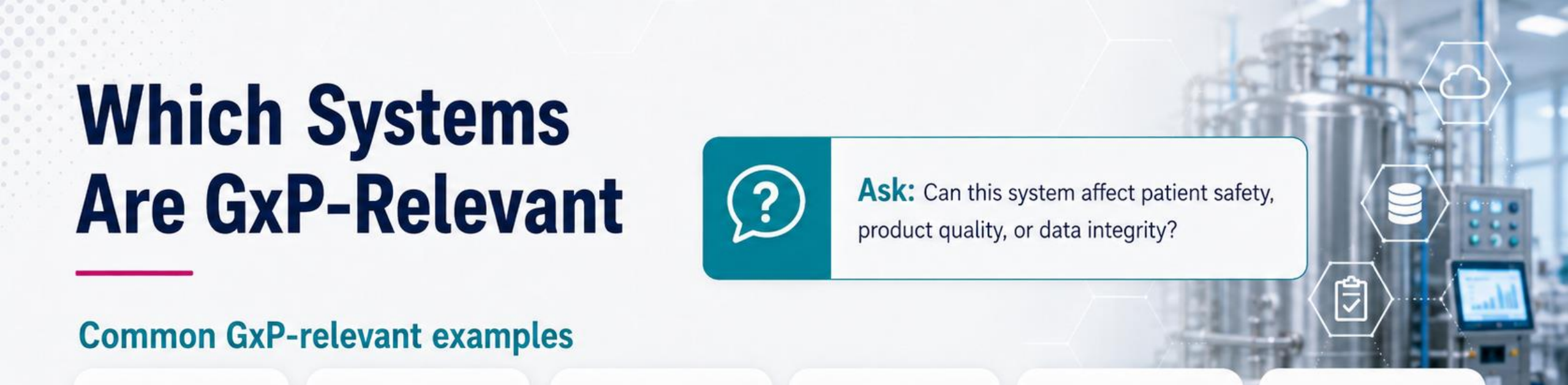
Evidence is documented

Validation decisions can be reviewed and defended

Goal: documented confidence in patient safety, product quality, and data integrity

Which Systems Are GxP-Relevant

Ask: Can this system affect patient safety, product quality, or data integrity?



Common GxP-relevant examples

LIMS

Sample and result management

eQMS

Deviations, CAPA, change control

MES / SCADA

Manufacturing execution and control

ERP quality modules

Batch, inventory, release data

Chromatography / CDS

Analytical data acquisition

Stability / validation tools

Studies, protocols, reports

If the answer is yes, document the impact and define the right validation depth.

Intended-Use Statement

Start validation by defining exactly what the system is expected to do in the regulated process.

Include these core elements

Purpose	Why the system is used
Process	Which workflow it supports
Users	Who will use and approve
Data	Inputs, outputs, and interfaces
Boundaries	In scope and out of scope
Success criteria	What acceptable performance looks like

Example

A LIMS used for QC sample login, result entry, review, approval, and reporting.

Initial GxP Impact Assessment

Use an early impact assessment to decide whether the system needs formal validation and how much control is required.

Key questions

Regulated process?
Does it support a GxP activity?

→

Quality decision?
Can it influence approval or release decisions?

→

GxP records?
Does it create, store, or process critical records?

→

Critical control?
Can it control equipment or critical parameters?

Possible outcome | Low, medium, or high GxP impact — with documented rationale and validation depth

Patient, Product, and Data Risks

Risk assessment should show what could go wrong, what the impact would be, and how the risk will be controlled.

Patient risk

- Wrong clinical or release decision
- Delayed or missed safety action
- Potential impact on patient well-being

Product risk

- Incorrect settings or calculations
- Mix-up, defect, or release error
- Failure to meet specifications

Data risk

- Unauthorized changes
- Missing audit trail or records
- Loss, inaccuracy, or incomplete data

Rate severity, likelihood, and detectability — then define controls and testing.

Regulatory Framework

CSV programs are built by combining regulations, guidance, and risk-management principles.

21 CFR Part 11

Electronic records and electronic signatures

EU GMP Annex 11

Computerized systems in GMP operations

GAMP 5

Risk-based industry guidance for lifecycle control

ICH Q9

Quality risk management principles

Use all four together: requirements, lifecycle control, and documented risk-based decisions

21 CFR Part 11

Part 11 focuses on trustworthy electronic records and reliable electronic signatures.

Key expectations

Validated systems

Records must be accurate, reliable, and consistent

Access control

Only authorized users can create or change records

Audit trails

Changes should be secure, time-stamped, and reviewable

Electronic signatures

Signatures must be linked to their records

Retention and retrieval

Records must remain available and readable

Focus: trustworthiness, authenticity, and integrity of electronic records

EU GMP Annex 11

Annex 11 defines expectations for computerized systems used in GMP environments.

Key expectations

Validated applications

Systems should be fit for intended GMP use

Qualified infrastructure

Supporting platforms and environments must be controlled

Lifecycle risk management

Apply risk management from selection to retirement

Supplier oversight

Define responsibilities and evaluate service providers

Operational control

Manage incidents, changes, backup, and periodic review

Data and access control

Protect records, permissions, and audit trails

Focus: maintaining the validated state throughout the system lifecycle