



John Hannan LLC
ERPgo-live.com

A WORKING TOOL FOR LIFE SCIENCES ERP TEAMS

ERP Validation Checklist - 21 CFR Part 11

The controls auditors expect to see proven, a one-page risk traceability matrix, and a test-case template with four worked examples. Built for teams validating a new ERP, and for teams choosing one who want validation readiness scored before the contract is signed.

What is inside

1. What to validate and what to leave in UAT
2. The checklist - governance, IQ, OQ, PQ, data integrity, execution quality
3. Risk traceability matrix (template with examples)
4. Test-case template and four Part 11 test cases
5. Eight questions to ask ERP vendors before you shortlist
6. Common pitfalls, and how to use this in an ERP selection

Prepared by John Hannan LLC, a vendor-neutral ERP selection firm. Free to use inside your company.

This is a practitioner's working tool, not legal or regulatory advice. Your quality unit owns the final validation plan.

Version 1.0 · October 2026 · Questions, or help scoring these controls in an ERP selection - erpgo-live.com/selection-help

1. What to validate, and what to leave in UAT

When a life sciences manufacturer asks whether its ERP is "validated for Part 11", the real question is whether electronic records, electronic signatures and data integrity controls hold up to audit in the way the system is used every day. 21 CFR Part 11 sets the conditions under which FDA accepts electronic records and electronic signatures in place of paper for records its regulations require, the predicate rules such as 21 CFR 210 and 211 for drugs and 820 for devices. In an ERP that means validation, limited and role-based access, identities unique to one person, reauthentication at the moment of signing, secure time-stamped audit trails that never obscure earlier entries, accurate and complete copies in human-readable form, and records protected for their retention period. Those controls are proven in Operational Qualification (OQ) and Performance Qualification (PQ), with traceability back to requirements under a Validation Master Plan (VMP).

The most common failure is scope that balloons. Convenience features get dragged into validation, the project slows, and the controls that matter get less attention. Keep validation on compliance-critical and product-quality-critical functions, and use a simple severity-by-likelihood risk matrix to decide how much rigor each control needs. This risk-based, critical-thinking approach is consistent with GAMP 5 and with FDA's Computer Software Assurance guidance.

Risk	Assurance	Examples
High	Scripted tests in IQ, OQ or PQ with objective evidence	Electronic signatures (identity, meaning, time, reauthentication). Audit trails for create, modify and delete. Lockouts, inactivity timeouts, user deactivation, release permissions, record integrity and tamper evidence. GMP-relevant flows such as receiving by lot with quarantine and release, picking restrictions for nonconforming items, label printing tied to traceability, QC sampling that drives accept or reject.
Medium	Moderate assurance - targeted scripts or configuration checks with evidence	Controlled reports used in GMP decisions. Role changes and permission sets. Integrations that carry quality data.
Low	Configuration checks or User Acceptance Testing (UAT)	Sync-complete notifications. Convenience dashboards. Non-regulated custom reports, unless they directly drive GMP decisions.

Maintain a risk log and keep every requirement traceable to IQ, OQ or PQ, or to UAT, so the scope can be defended in an audit and in a budget review.

2. The checklist

Tick each line when the control is in place and the evidence is filed. The right-hand column says what an auditor, or a selection team scoring a vendor demo, should expect to see.

A. Governance and documents, from day one

Control or deliverable	What to look for
☐ Validation Master Plan (VMP)	Defines the lifecycle, IQ, OQ and PQ, roles, deliverables and a traceability matrix from requirements to tests and evidence.
☐ Risk assessment SOP and risk traceability matrix	Links each specification to a risk rating and an assurance level (see section 3).
☐ Change management SOP	Ticketing, code review and approvals, release notes. Protects the validated state after go-live.
☐ Document control SOP	Numbering, approvals, revision control and obsolescence, so nobody runs the wrong script.
☐ Data storage, backup and recovery SOP	Backup cadence, retention, restore testing and audit trails, for example daily full plus log backups and storage lifecycle policies.

B. Installation Qualification (IQ)

Control or deliverable	What to look for
☐ Environment documented and approved	Versions, tenants, integrations and infrastructure match the approved design.
☐ Identity provider connected	Single sign-on or directory integration in place; service accounts documented.
☐ Roles and permissions loaded	Role design approved; least privilege shown in a permissions report.
☐ Time synchronization configured	Reliable, consistent timestamps across environments.
☐ Backups scheduled per SOP	Schedule, retention and ownership match the backup SOP.
☐ Evidence collected	Screens, configuration exports and logs filed against the IQ protocol.

C. Operational Qualification (OQ) - Part 11 core controls

Control or deliverable	What to look for
☐ Electronic signature linkage and tamper evidence	Sign a record. The signature shows the signer's printed name, the date and time, and the meaning (review, approval, release). The signature is linked to the record so it cannot be excised, copied or transferred, for example by a content hash, and an attempted alteration is detected.
☐ Reauthentication before e-signature	After login, applying a regulated signature prompts for at least one signature component again (a password or MFA), and the first signing in a session uses all components.
☐ Credential strength and lockouts	Password complexity enforced. Repeated failed attempts (for example ten) lock the account and log an event.
☐ Session management	Inactivity (for example thirty minutes) requires sign-in again before access continues.

Control or deliverable	What to look for
☐ User lifecycle	No duplicate usernames. A deactivated user cannot log in, and the denial is audit-trailed in the ERP and the identity provider.
☐ Audit trail content and readability	Create, modify and delete captured with who, what and when, and the reason for change where a predicate rule or your SOP requires it. Earlier entries are never obscured. Records viewable and printable in human-readable form.

D. Performance Qualification (PQ) - process fit in your workflows

Control or deliverable	What to look for
☐ Receiving and status control	PO to receipt to quarantine to release. Lot and expiry captured, status transitions enforced, rejection evidenced where required.
☐ Picking restrictions	Nonconforming or quarantined inventory cannot be picked.
☐ Labeling and license plate printing	Where labels drive traceability, printing is controlled and traceable.
☐ QC sampling and inspection	Where results drive accept or reject decisions (AQL or equivalent), the business rule and expected decision logic are documented and proven.
☐ Batch and electronic batch record release	Release controlled by authorized roles (for example QA) with signatures and timestamps.

E. Data integrity, retention and restoration

Control or deliverable	What to look for
☐ Backups executed per SOP	Daily full plus frequent log backups, with logs retained.
☐ Restore tested	At least one documented restore scenario as objective evidence.
☐ Audit trails retained for the defined lifecycle	Retention period set and demonstrated.
☐ Access to scripts and logs restricted	Identity and access management with MFA; access is traceable.

F. Execution quality (ALCOA+)

Control or deliverable	What to look for
☐ Approved, version-controlled scripts	The script run is the approved revision.
☐ Actual outcomes recorded	Results say what happened, not only Pass.
☐ Dated screenshots and logs attached	Evidence is attributable, legible, contemporaneous, original and accurate.
☐ Deviations raised, never worked around	If behavior differs from the expected result, stop and raise a deviation. Never edit a script mid-run.

3. Risk traceability matrix

One page that keeps every requirement covered to closure, in line with the V-model. Each requirement carries a risk rating, an assurance level, a test, its evidence, a result and any deviation. Three example rows are filled in; the rest are yours (leave nine blank rows).

Req ID	Requirement	Risk	Assurance	Test ID	Evidence	Result	Deviation
R-011	Regulated signatures require reauthentication at the moment of signing	H	OQ	T-OQ-02	Screens 02-a to 02-d, audit log extract	Pass	-
R-014	Inactive sessions end after 30 minutes	H	OQ	T-OQ-05	Screen 05-a, timestamped	Pass	-
R-032	Nonconforming inventory cannot be picked	H	PQ	T-PQ-03	Pick attempt screen, status report	Fail	DEV-004

Rating guide - Risk is H, M or L. Assurance is IQ, OQ, PQ or UAT. High means a failure could affect product quality, patient safety or the integrity of a regulated record. Medium means a failure would be caught by another control or does not touch a regulated decision. Low means convenience or cosmetics. Assurance follows risk - High gets scripted tests with objective evidence, Medium gets moderate assurance, Low goes to configuration checks or UAT.

4. Test-case template

Use one of these per test. Record what actually happened, attach dated evidence, and raise a deviation rather than reinterpreting a result.

Field	Entry
Test ID	
Title	
Requirement(s)	
Risk and assurance level	
Precondition	
Steps	
Expected result	
Actual result	
Evidence (screens, logs, exports)	
Result (Pass, Fail) and deviation number	
Tester, date	
Reviewer, date	

Four worked Part 11 test cases

Starter protocol excerpts you can adapt. Each proves a control that auditors ask about first.

Test ID	T-OQ-02
Title	Reauthentication before e-signature
Precondition	Tester is logged in with a role authorized to e-sign GMP records.
Steps	1. Open a controlled record. 2. Select Sign. 3. Provide credentials or MFA when prompted.
Expected result	The system prompts for reauthentication. The signature applies only after successful reauthentication. The audit trail logs name, date and time, and meaning.

Test ID	T-OQ-05
Title	Session timeout
Precondition	Tester is logged in.
Steps	1. Remain idle for 30 minutes. 2. Attempt navigation.
Expected result	Access is blocked until reauthentication, with no data loss.

Test ID	T-OQ-07
Title	User deactivation
Precondition	A test user exists in the identity provider and in the ERP.
Steps	1. Deactivate the test user in the identity provider. 2. Attempt login and use.
Expected result	Login is denied. The denial is logged in both the ERP and identity-provider audit logs.

Test ID	T-OQ-09
Title	Record integrity and print
Precondition	A signed record exists.
Steps	1. Retrieve the signed record. 2. Print it. 3. Verify the human-readable content and the signature details. 4. Alter the record in a test copy and re-check.
Expected result	The print shows unaltered, human-readable content and signature details. Alteration is detected, for example by a hash mismatch.

5. Eight questions to ask ERP vendors before you shortlist

Validation cost and time balloon when you start from zero. Put these to every vendor in the RFP, and make the answers part of the scorecard.

#	Question	A good answer looks like
1	What validation documentation do you provide out of the box, such as requirements mapping, test scripts and evidence templates?	A validation accelerator package, with sample IQ, OQ and PQ scripts you can inspect before signing.
2	Which parts of the solution are pre-validated by you, and which must be validated by us based on our configuration?	A clear shared-responsibility summary you can include in your own compliance documentation.
3	How do you support validation for updates, patches and new releases, and what is your recommended approach for keeping the validated state?	Release notes with impact assessments, a regression test pack, and a say in release timing for regulated customers.
4	Can you provide sample validation deliverables from similar regulated clients, with sensitive details removed?	Real examples, not a brochure.
5	How are electronic signatures implemented, and does signing require reauthentication at the moment of signing?	A live demo on your record types, with the signature manifestation and the audit trail entry shown.
6	What does the audit trail capture, who can view it, can anyone modify it, and how long is it retained?	Create, modify and delete with who, what, when and reason, read-only to users, retained for the record's lifecycle, exportable for inspections.
7	What are your password, lockout, session-timeout and user-deactivation controls, and can we configure them?	Configurable policies, with deactivation flowing from your identity provider and logged in both places.
8	What retention, legal hold, backup and restore options exist, and when was a restore last tested?	A documented restore test and retention policies you can set by record type.

6. Common pitfalls, and how to avoid them

Pitfall	What goes wrong	What to do instead
Validation bloat	Business timing and convenience features get folded into Part 11 scope. The project slows and attention leaves the controls that matter.	Keep them in UAT unless they drive GMP decisions. Use the risk matrix to defend scope.
Weak change control	Changes land without tickets, review or traceable approvals, and the validated state erodes.	Enforce review approvals and release notes. Treat every change as a potential revalidation trigger.
Backups without restorations	Backups alone do not prove data is available and retrievable.	Include a documented restore test and retain the logs.
Document chaos	Unclear numbering and ownership; people run the wrong script.	Lock down document control and approvals before the first test runs.

Using this checklist in an ERP selection

The cheapest time to settle validation is before the contract is signed. In a vendor-neutral selection, the controls in section 2 become scored requirements, the questions in section 5 go into the RFP, the test cases in section 4 become scripted demo scenarios each vendor must perform on your data, and the vendor's validation package, Part 11 controls and audit-readiness evidence are weighed alongside fit and cost. The validation commitments then go into the contract and statement of work, so IQ, OQ and PQ start from a known position rather than from zero.

John Hannan LLC runs vendor-neutral ERP selection programs for life sciences, manufacturing and distribution companies. We do not sell software and we take no referral fees from vendors. If you are choosing an ERP for a validated environment, we can make Part 11 controls, validation support and vendor evidence part of the scorecard, turn requirements into demo scripts that show IQ, OQ and PQ readiness, and write the validation commitments into the SOW.

Talk to John about your ERP program ·
erpgo-live.com/selection-help · (570) 71-JHLLC · hello@erpgo-live.com

Related reading on erpgo-live.com - [How to Accomplish FDA Validation for ERP Software](#) · [Understanding 21 CFR Part 11 Compliance when selecting a new ERP System](#) · [Life Sciences ERP Software Selection, 2026 Buyer's Guide for Validated \(GxP-Ready\) Environments](#).

This document is a practitioner's working tool and does not constitute legal or regulatory advice. Your quality unit owns the validation plan and the final determination of scope. 21 CFR Part 11 is a regulation of the U.S. Food and Drug Administration; consult the current text and FDA guidance.