QMSdesk™

www.qmsdesk.com
info@akatalyst.com
India +91 77600 78606
Dubai +971 50 280 1688

REGULATION CHECKLIST

Computer Software Assurance: principle-by-principle checklist

Reviewed by Abdul Azam, Founder & CEO, 25 years in regulated life-sciences quality. Last reviewed September 26, 2026.

> QMSdesk is designed to support these recommendations. FDA's Computer Software Assurance guidance (version issued February 3, 2026) is nonbinding. Validation for your intended use is established by you, in your environment; the last column is yours to complete. This checklist is general information, not legal or regulatory advice.

The CSA principle map

CSA principle (paraphrased)	How QMSdesk supports it	What you still own	Your evidence
Validate for intended use (ISO 13485 §4.1.6, §7.5.6, §7.6 via QMSR). FDA recommends looking at each feature, function or operation (guidance §V.A.1)	A signed System Boundary Statement, available at any time, shows which modules you run in QMSdesk. If you run Audits or Suppliers elsewhere, they read "managed outside QMSdesk". Your written validation scope names what our validation covers.	The intended-use statement for each function you use, and the decision that it forms part of your quality management system.	
Decide whether each function is high process risk (guidance §V.A.2)	Keep your risk determination for each function as a controlled document, with signed review and approval.	Your risk determination, for your processes and your products. FDA's examples are a guide, not your conclusion.	
Build on the vendor's work (purchasing controls) (guidance §V.A.5)	QMSdesk's core platform is validated under a QA-approved Validation Summary Report. We'll walk you through the full record under a mutual NDA.	Your supplier assessment, your acceptance of our evidence, and the purchasing-control record.	
Assess the vendor's data-integrity controls (guidance §V.A.5)	Every audit-trail entry is SHA-256 hash-chained, and the database keeps the log insert-only. Daily jobs re-verify every chain and check that every signature still resolves to its record. Signatures require re-authentication and record their meaning. Access is governed by granular permission keys. Records are never hard-deleted, and retention floors run to 7, 10, 15 or 30 years.	Confirming these controls meet your requirements, and running the procedures around them, such as access reviews and periodic audit-trail review. See the Trust Center.	
Use unscripted testing where it suits the risk (guidance §V.A.4)	Implementation Mode in your real tenant: once implementation testing opens, every module you run works, so your people can run scenario, error-guessing and exploratory tests on their own workflows. The test records are kept as evidence and are left out of your live KPIs by default.	The test objectives, pass/fail criteria and the testing itself.	

CSA principle (paraphrased)	How QMSdesk supports it	What you still own	Your evidence
Consider scripted testing for higher-risk functions (guidance §V.A.4)	The same tenant, the same configuration you'll go live on. Go-live readiness checks are drawn from the audit trail, for example a workflow step exercised for each event type you've switched on.	The testing approach for each function you rate high risk (scripted, unscripted or a mix), and approval of the test plan where appropriate.	
Establish the record, digitally where you can (guidance §V.A.6)	The audit trail records who did what and when. Two separately signed go-live attestations cover technical and quality readiness. Keep your validation plan and summary as controlled documents, with signed review and approval.	The conclusion statement declaring the software acceptable for your intended use, and its approval.	
Keep the validated state (guidance §V, §V.A.3)	After go-live, a validation-affecting setting can't be written until an approved change control reaches implementation, and the revalidation flag clears only by a recorded decision when that change control closes. Workflows are versioned definitions that administrators can't edit.	Assessing each QMSdesk update, and each of your own changes, against your intended use. For PMA or HDE devices, deciding whether a software change needs a 30-day notice or an annual report.	
Part 11 generally applies to Part 820 records you keep electronically (guidance §V.B)	Controls for electronic records and signatures, detailed on our 21 CFR Part 11 page.	Your procedures, and the §11.100(c) certification to FDA that the electronic signatures in your system are intended to be the legally binding equivalent of traditional handwritten signatures.	