QMSdesk™

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

REGULATION CHECKLIST

21 CFR Part 11: clause-by-clause checklist

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

> QMSdesk is designed to support the controls described in the second column. Rows marked outside QMSdesk's scope or not applicable, and all procedures, are yours. Compliance is established in your environment, for your intended use; the last column is yours to complete. This checklist is general information, not legal or regulatory advice.

Subpart B: electronic records

Requirement (paraphrased)	How QMSdesk supports it	Evidence the system produces	What you still own	Your evidence
§11.10(a) Validate systems for accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.	QMSdesk's core platform is validated under a QA-approved Validation Summary Report. A SHA-256 hash chain makes an altered or deleted audit-trail entry detectable. Go-live takes two separately signed attestations.	Validation Summary Report, walked through with you under a mutual NDA; daily chain-verification results; signed go-live attestations	Validating QMSdesk for your intended use, in your environment, under a written validation scope	
§11.10(b) Generate accurate and complete copies, human readable and electronic, for FDA inspection and copying.	PDF and Excel reports; controlled copies with a signature log; closure records for closed events; audit-trail export; read-only Inspection View accounts that can export.	Controlled-copy and closure-record downloads are logged, as is every download or export from an Inspection View account	Confirming the copies you provide are complete for each predicate-rule record	
§11.10(c) Protect records for accurate, ready retrieval throughout the retention period.	A retention floor set by your regulatory profiles (7, 10, 15 or 30 years). Records are archived, never hard-deleted. A daily job checks that every signature still resolves to its record and reports any it can't confirm.	Retention sweep log; signature-linkage results	Confirming the retention floor covers every predicate rule you work under	
§11.10(d) Limit system access to authorized individuals.	One person per account; multi-factor authentication for the tenant or by role; SAML single sign-on; lockout after failed attempts; an inactivity timeout and a maximum session length. Break-glass and vendor support access are time-boxed and logged.	Access events in the audit trail; periodic access reviews	Granting and removing access as people join, move and leave. A policy that forbids shared accounts	

Requirement (paraphrased)	How QMSdesk supports it	Evidence the system produces	What you still own	Your evidence
§11.10(e) Secure, computer-generated, time-stamped audit trails that independently record operator entries and actions that create, modify or delete records. Changes must not obscure earlier entries. Keep the trail at least as long as the record must be kept, and make it available to FDA for review and copying.	Every entry is SHA-256 hash-chained to the one before it, and the database keeps the log insert-only for every connection. Entries capture who, what, which record, old and new values, the reason and the time. Records raised in error are cancelled with a signed reason, never hard-deleted.	Audit trail and export; daily chain verification; signed periodic audit-trail review	Reviewing the audit trail on the cadence your own SOP sets	
§11.10(f) Operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Every event and CAPA workflow is one versioned definition that rejects out-of-sequence status changes, and administrators can't edit its steps or transitions. CAPA effectiveness verification can't be skipped.	The step history of every record	Confirming each workflow's sequence matches your procedures	
§11.10(g) Authority checks: only authorized people use the system, sign, access input or output devices, alter records or perform the operation.	Access is granted through individual permission keys from one controlled catalog. Signature authority is validated before a signature is accepted. Segregation of duties is enforced at signing, and the Administrator holds no record-approval authority.	Role assignments, signed and audit-trailed, time-bound, signed segregation-of-duties waivers	Deciding who holds which role	
§11.10(h) Device checks on the validity of the source of data input or operational instructions, as appropriate.	Outside QMSdesk's scope.	—	Your procedure: decide whether any device checks apply to your use	
§11.10(i) People who develop, maintain or use the system have the education, training and experience for their tasks.	For your users: training assigned on new hire and role change, quizzes, practical and competency assessments. Overdue training for a GxP-critical role opens a risk.	Training and competency records, signed	Deciding who is qualified, and the content of your training. Assessing our team in your supplier assessment	
§11.10(j) Written policies that hold people accountable for actions under their electronic signatures.	Your procedure. QMSdesk can control the policy as a document and assign it with a signed "read and understood" acknowledgment.	Signed acknowledgments	Writing the policy and enforcing it	

Requirement (paraphrased)	How QMSdesk supports it	Evidence the system produces	What you still own	Your evidence
§11.10(k) Controls over system documentation: (1) its distribution, access and use; (2) revision and change control with an audit trail.	Document control for your SOPs and system documentation: signed lifecycle, controlled copies with every download logged, restricted documents. After go-live, a validation-affecting setting changes only through approved change control.	Document versions and signatures, change-control records	Your system documentation and the procedures that govern it	
§11.30 Open systems: §11.10 controls plus measures such as document encryption and digital-signature standards.	Your administrators govern access to your tenant, and single sign-on can run through your own identity provider. Vendor support access is time-boxed, visible to you and can never sign.	Support-access grants, logged	Classifying the system as closed or open, and adding any extra measures an open system needs	
§11.50 Signed records show the signer's printed name, the date and time, and the meaning of the signature, under the same controls as the record and in any human-readable form.	Every signature records who signed, when, and its meaning, from a controlled vocabulary of signature meanings set by the system for each step.	Signature log on controlled copies, full signature manifest on event closure records	Confirming the meanings match the signatures your procedures require	
§11.70 Signatures are linked to their records so they can't be excised, copied or otherwise transferred to falsify a record by ordinary means.	Each signature is bound to its record by a content hash of what was signed. A daily job re-checks every link and reports anything it can't confirm as unverified.	Daily signature-linkage results	Including the link check in your validation	

Subpart C: electronic signatures

Requirement	How QMSdesk supports it	Evidence the system produces	What you still own	Your evidence
§11.100(a) Each signature is unique to one person and is not reused by, or reassigned to, anyone else.	One person per account, and user IDs are never reissued. Break-glass and vendor support access can never sign.	Every signature attributed to one identity	A policy that forbids shared accounts	
§11.100(b) Verify a person's identity before establishing their electronic signature.	Your procedure. With single sign-on, identity is established in your identity provider.	—	Verifying each person's identity before you create their account	

Requirement	How QMSdesk supports it	Evidence the system produces	What you still own	Your evidence
§11.100(c) Certify to FDA that the electronic signatures in your system are intended to be the legally binding equivalent of handwritten signatures.	Outside QMSdesk's scope.	—	The certification, signed by hand and submitted to FDA on paper or electronically, and any further certification FDA asks for	
§11.200(a)(1) Non-biometric signatures use at least two distinct components, such as an ID and a password, with rules for signing within one session and across sessions.	Every signature re-authenticates the signer, with multi-factor authentication at signing when your tenant requires it. No signature relies on the sign-in alone.	Signature records	Confirming in your validation that your signing configuration meets §11.200(a)(1)(i) and (ii)	
§11.200(a)(2) Signatures are used only by their genuine owners.	Lockout after failed attempts, single-use password reset links and multi-factor authentication.	Locks and unlocks in the audit trail	Your accountability policy (§11.10(j)) and training	
§11.200(a)(3) Misuse of someone's signature requires two or more people to collaborate.	The Administrator holds no record-approval authority. Vendor support access needs a second operator's authorization, and full administrative access needs your consent.	Support-access grants, logged	Your procedures for issuing credentials and administering accounts	
§11.200(b) Biometric signatures can only be used by their genuine owners.	Not applicable: QMSdesk signatures aren't biometric.	—	—	
§11.300(a) Each ID and password combination is unique.	One account per person, and IDs are never reissued.	User records	A policy that forbids shared accounts, and unique identities in your identity provider if you use single sign-on	
§11.300(b) ID and password issuance is periodically checked, recalled or revised, for example through password aging.	Configurable password expiry and password history, plus periodic access reviews.	Access-review records	Setting the policy and running the reviews	
§11.300(c) Loss management for lost, stolen or compromised tokens and devices.	An administrator can deactivate an account at once, and the deactivation is recorded.	Deactivation records	Your loss-management procedure, including second-factor devices and your identity provider's tokens	
§11.300(d) Safeguards against unauthorized use, with immediate, urgent reporting of attempts to your security unit and, as appropriate, to management.	Lockout after a set number of failed attempts. Every lock and unlock is recorded in the audit trail.	Audit-trail entries	The urgent reporting route to your security unit and management	

Requirement	How QMSdesk supports it	Evidence the system produces	What you still own	Your evidence
§11.300(e) Initial and periodic testing of tokens and cards.	Outside QMSdesk's scope.	—	Your procedure, and your identity provider's	