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

CAPABILITY OVERVIEW

QMSdesk™ capability overview

eQMS features in QMSdesk, grouped by module: documents, events, CAPA, change, training, risk, audits, suppliers and oversight. In every tier.

Bring your eQMS requirements checklist. QMSdesk™'s eQMS features are listed below, grouped by module, and every tier includes all of them.

How to use this QMS software features list

Each group opens with what the module changes for you, then lists what's in it, one line per feature, ready to paste into your eQMS requirements checklist. Each module has its own page at www.qmsdesk.com/platform.

eQMS features by quality module

Document control

The current version, with the right signatures behind it.

- Lifecycle: Draft, then Review, then Approval, then Approved, then Effective, then Superseded, Obsolete or Retired
- Signatures at authoring, review and approval
- Reviewers request changes (an attributed comment) or reject (a signed finding); any return goes back to Draft for full re-review
- Author, reviewer and approver kept separate at signing; two independent approvers for high-criticality documents
- Effective-date grace period, 14 days by default, with a signed early release
- Training assigned when a document is approved
- Controlled-copy PDF with a "CONTROLLED COPY" banner and signature log
- Downloads logged, and blocked if logging fails
- Typed cross-references, a "Referenced by" view and stale-reference flags
- Periodic review tasks; a risk opens after 30 days overdue
- Reference documents (standards, guidance, CVs, quality agreements) with provenance, currency checks and a "not internally approved" banner
- Restricted documents hidden from lists, search, counts and exports for anyone without rights
- Licensed standards viewable in the app, with download suppressed
- Author in the editor or upload a source file
- Migration import with one signed attestation per batch and a permanent "Migrated" badge

Quality events

Every event on its own enforced workflow, from report to closure.

- Six event workflows: incident, deviation, nonconformance, complaint, OOS/OOT and supplier issue
- Anyone can report an event; control applies from triage onward

- Deviations routed by severity: minor on a short path with one signature; major and critical through containment, investigation, a signed CAPA decision and QA approval
- Nonconformance disposition signed: reject, rework, use-as-is (with technical rationale) or return
- Incident containment required for major and critical incidents
- Complaints: acknowledgment tracked against a 3-business-day SLA, a signed reportability review, a signed CAPA decision and a customer response
- OOS/OOT: a mandatory two-phase investigation following FDA's OOS guidance (Revision 1, May 2022)
- Supplier issue (SCAR): signed response review, verification and closure that sets supplier status
- Profile workflows: GLP study deviation, GLP QAU finding, and patient safety event (always raises a CAPA)
- Profile event types, from batch deviation and MDR vigilance to protocol deviation and ATMP process nonconformance
- Records raised in error cancelled with a signed reason, never hard-deleted
- A missed deadline escalates but never blocks; a late step records its delay reason
- Closure Record PDF with the full signature manifest, available once an event closes

CAPA

A CAPA is something you commit to do, so it's a record in its own right.

- A peer of change control, raised from an event, a trend, an audit or a management review
- Lifecycle: Reported, then Investigation, then Action plan review, then Implementation, then Verification, then Closed
- Effectiveness verification that can't be skipped
- Action items, each with its own evidence and QA review (Moderate, Major and Critical CAPAs)
- The investigator can't sign the action-plan review
- The approved action plan raises the linked change control and training
- Scheduled effectiveness checks after closure, at the interval you set
- A failed check raises a new, linked CAPA; the signed one is never reopened
- A risk assessed at your CAPA-trigger level raises a linked CAPA automatically
- An event's CAPA is raised by its signed CAPA decision, in the same transaction

Change control

The right eyes on every change, scaled to its risk.

- Lifecycle: Draft, then Triage, then Assessment, then Approval, then Implementation, then Verification, then Closed, with On hold, Rejected and Cancelled
- Risk-based approval routing: high-impact changes go to the Change Manager and the Quality Manager
- Classification can raise the tier but never lower it
- Approvers can be added, never removed
- The requester can't approve; the implementer can't verify
- Change actions for implementation
- Post-go-live configuration changes run as ordinary change controls

Training and competency

The right people trained, with the evidence to show it.

- Four ways to complete: signed acknowledgment, quiz graded against a frozen snapshot, practical assessment signed by a qualified assessor, external certificate
- Automatic assignment on document approval, change implementation, CAPA plan, new hire, role change and department change

- Recurring refreshers, overdue flags and digests
- Signed, time-limited waivers and equivalencies
- Competency assessments by qualified assessors
- Overdue training for a GxP-critical role opens a risk
- Training transcripts per person

Risk management

Proactive, risk-based quality: risk decides what happens next.

- Lifecycle: Identified, then Assessed (signed), then Mitigation planned, then Mitigated (signed residual), then Monitoring, then Accepted (residual risk accepted, signed) or Closed
- Likelihood × impact on a 5×5 matrix, or FMEA RPN
- Your own thresholds on the 5×5 matrix
- Severity dominance: a maximum-severity risk never scores below High
- Built on ISO 14971 and ICH Q9(R1) principles
- ISO 14971 control model: implementing and verifying kept separate, residual risk scored only after verification
- Control taxonomy following ISO 14971 §7.1, and new hazards from a control raised as risks
- Built-in risk templates, plus your own
- Risks opened automatically by an expired supplier certificate, a document review 30 days overdue, or overdue GxP training
- An ineffective CAPA sends its risk back for re-assessment

Audit management

Audits that stay independent, and findings that go somewhere.

- Lifecycle: Planned, then Scheduled, then In progress, then Completed (lead auditor signs), then Approved (management signs), then Closed
- Auditors can't audit their own department; the lead auditor can't approve their own report
- Critical findings raise a nonconformance and a risk; major findings raise a nonconformance; optional linked CAPA
- One register of findings across every audit
- Opportunities for improvement and positive observations, without finding consequences
- Audit programs, templates and auditor qualification profiles
- Inspection View: time-boxed, read-only accounts for inspectors that can still export, with every access logged

Supplier quality

Supplier risk that follows real performance.

- Lifecycle: Prospect, then Under evaluation, then Conditionally approved or Approved, then Active, then Suspended or Disqualified, with signed decisions
- Risk tiers (Critical, Key, Standard) set qualification gates, completeness gates and 6-, 12- or 24-month reviews
- Approved Supplier List, with conditional approvals marked
- Certificate expiry alerts at 90, 60 and 30 days, and a risk opened on expiry
- Periodic re-evaluation tasks and a supplier scorecard
- Two rejected SCAR responses raise the supplier to the Critical tier
- Single-use SCAR link: no account, no seat, two fields to answer, expires on use, attributed in your audit trail

Management review

Minutes and evidence that agree.

- A signed, frozen snapshot of the quality system as of the period end, never edited or recomputed
- Reviews scheduled, run and closed, with minutes and decisions signed at closure
- Follow-up actions assignable after closure
- SoD waivers included in the review pack automatically

Reporting and analytics

The state of your quality system, any day.

- Command Center with five views: Executive Pulse, Inspection Readiness, Risk Command, Training Intelligence and Notification Activity
- Every figure opens the records behind it
- My Work: each person's open tasks, deadlines and activity
- Review queue: everything awaiting your signature, across modules
- Global search that respects permissions and site scope
- Event trending, with OOS lab-error trends by method, analyst and instrument
- PDF and Excel reports, plus weekly scheduled reports
- In-app inbox as the system of record; notifications never deleted
- Navigation grouped into My Work, Operations, Oversight and Administration
- Reminders before a due date, then widening escalation to coordinator and Quality Manager

Platform services behind every module

Audit trail and e-signatures

A tamper-evident trail behind every record.

- Every audit-trail entry SHA-256 hash-chained to the one before it
- Audit-log immutability enforced at the database layer
- Daily chain verification, on demand too; only a genuine break fails
- Daily check that every signature still resolves to its record
- Signed periodic audit-trail review over a risk-focused view
- A controlled vocabulary of signature meanings
- Re-authentication on every signature, with MFA where required
- Signature and record change committed in one transaction

Regulatory profiles

Built from the regulations up.

- 12 regulatory profiles, built from a registry of 27 regulations, standards and guidelines
- Profiles chosen directly at onboarding, several at once
- Event types, roles and required fields combined; the longest retention floor and the tightest step deadlines apply
- Electronic signature wherever any profile requires it
- Add-only for the life of your tenant

Workflow engine

Your procedures, enforced step by step.

- Eight connected quality objects: document, event, CAPA, risk, change, audit, training and supplier
- One versioned definition per workflow, read alike by the interface, API and validator
- Each step declares its required fields, electronic signature and SLA
- Steps and transitions locked; direct status writes rejected
- A daily check flags any live workflow behind its current definition
- New required fields apply to new records only
- Decision-driven cascades committed in the same transaction as the signed decision
- Typed, attributed links between any records; a removed link is kept
- Cascades into a module managed elsewhere suppressed and logged
- Scheduled jobs for due dates, expiries, periodic reviews, retention and integrity checks
- Configurable numbering by prefix, year, site, department and counter, never reissued

Implementation and go-live

From setup to go-live, in your real tenant.

- Six-stage Configuration Runway
- Implementation Mode: modules locked during setup, a banner for every role
- Testing in your real tenant, with the records kept as evidence
- Implementation-era data kept out of live KPIs, and watermarked on PDF reports
- Go-live gate with evidence-based checks and two signed attestations
- Change control on validation-affecting settings after go-live
- Document migration with a signed batch attestation

Access and governance

Authority where it belongs.

- 9 core roles, plus the roles each profile adds
- Granular permission keys; authorization checks the key, never the role name
- The Administrator holds no record-approval authority
- Segregation of duties checked when each signature is applied
- Time-bound SoD waivers; the beneficiary can't approve their own
- Break-glass access: granted, logged, time-boxed, reviewed, and never able to sign
- Delegations for cover and periodic access reviews
- Vendor support access: 7 days per grant (one extension, 30 days at most), authorized by a second operator, visible to you, never able to sign
- Custom roles through the API, with no self-escalation and signed changes
- One person per account; user IDs never reissued
- Password history, lockout, MFA by tenant or role, an inactivity timeout and a maximum session length
- Tenant isolation by row-level security in the database

Records and retention

Kept for the longest period any of your profiles sets.

- One retention clock per tenant, at the longest floor your profiles set: 7, 10, 15 or 30 years; your SOPs can set it longer

- Archived at the end of retention, never hard-deleted
- Audits or suppliers can be marked "managed outside QMSdesk"
- A suspended module stays readable and exportable
- A signed System Boundary Statement, available at any time

Integration and tenant

Sign in the way you already do, and connect your other systems.

- SAML single sign-on with Okta, Microsoft Entra ID, Google Workspace or custom SAML
- REST API for audits, changes, documents, events, risks, suppliers and training
- OAuth client credentials, API keys and OpenAPI documentation; integrations act but never sign
- Site tokens in numbering, and site scope in search
- Your logo in the app and on controlled-copy cover pages
- A custom sign-in domain, set up by our team

Every tier includes all of it

QMSdesk is priced by organization size, in three tiers: Early-Stage & Startup (1–25 users), Growth & Mid-Market (26–250) and Enterprise & Multi-Site (251 and above). Every module is in every tier, and growing past your band never locks anyone out. See pricing.