Software Validation Summary

Axiospec calibration management Prepared for the quality manager, validation lead, or IT reviewer evaluating Axiospec as a calibration system of record.

Document version 1.0. Last reviewed 2026-08-19. Published by CaliTech LLC, Knoxville, Tennessee.
Questions: support@axiospec.com, reply within one business day.

Read this first

This document is an **input to your validation record. It is not a validation record.**

Axiospec does not validate your instance, does not certify your compliance, and does not perform your qualification. Validation is a determination you make about your own intended use, your configuration, your procedures, and your people. Your registrar, assessor, or inspector decides whether you met it.

What this document gives you: a statement of intended use, a description of the data-integrity controls that exist in the product and how they are enforced, a checklist you can execute and sign in your own workspace, our change-management practice, and a plain list of what the software does not do.

Under GAMP 5 categorization, a configured multi-tenant SaaS register of this kind is normally treated as Category 4 (configured product). That means your validation effort is risk-based and leverages vendor documentation plus your own configuration and process testing. Confirm that categorization against your own procedure.

1. Intended use statement

Axiospec is a record-keeping system for measuring and test equipment. Its intended use is to:

- Maintain a register of instruments, including identity, manufacturer, model, serial number, location, site, and workspace-defined custom fields.
- Record calibration and verification events against those instruments, including as-found and as-left readings, nominal value, tolerance, result, environmental conditions, reference standard used, certificate number, service provider, and traceability reference.
- Record metrology fields used by ISO/IEC 17025 workflows: measurement uncertainty, coverage factor, confidence level, decision rule, conformity statement, and the reference standard's own certificate number.
- Identify the calibration status of each instrument and its next-due date, and surface overdue and due-soon instruments.
- Retain those records in an append-only, tamper-evident form with attribution and timestamps.
- Route calibration records through an optional two-person approval before they become effective.
- Produce a complete, human-readable and machine-readable export of the register and its history for audit.

Axiospec is **not** an accredited calibration laboratory and does not perform measurements. Every artifact the system produces carries this statement verbatim:

> "Calibration data recorded by workspace personnel. Axiospec is a record-keeping system, not an accredited calibration laboratory, and did not perform this measurement."

Axiospec is not medical device software and no claim of IEC 62304 relevance is made or implied. IEC 62304 governs software that is, or is part of, a medical device. A calibration register is a quality-system tool.

Which clauses drive the expectations on a system like this

Clause text for ISO standards is copyrighted, so the following are clause references with paraphrase, not quotations. Verify against your own licensed copy.

- **ISO 9001:2015 clause 7.1.5.2** (measurement traceability): equipment calibrated or verified at specified intervals against traceable standards, identifiable as to calibration status, safeguarded from invalidating adjustment, and an assessment of prior results when equipment is found unfit.
- **ISO 9001:2015 clause 7.5.3** (control of documented information): availability, protection against loss of integrity, control of access, storage and preservation, control of changes and version control, retention and disposition.
- **ISO 9001:2015 clause 8.4** and **ISO/IEC 17025:2017 clause 6.6** (externally provided products and services): you must evaluate and record your qualification of Axiospec as a supplier. This document is intended to be evidence for that record.
- **ISO/IEC 17025:2017 clause 6.4** (equipment), specifically 6.4.6 (calibration where accuracy or uncertainty affects validity), 6.4.8 (status labelling or coding so the user can readily identify calibration status or period of validity), and 6.4.13 (the required content of equipment records).
- **ISO/IEC 17025:2017 clause 7.11** (control of data and information management), specifically 7.11.2 (the information management system is validated for functionality, including interfaces) and 7.11.3 (protected from unauthorized access, safeguarded against tampering and loss, operated per specification, maintained to ensure data integrity, with failures and corrective actions recorded).
- **ISO 13485:2016 clause 4.1.6**: procedures for validating computer software used in the QMS, before initial use and after changes, with the approach proportionate to risk, and records maintained.
- **21 CFR Part 11**, where the calibration records are your regulated records of record: 11.10(a) validation, 11.10(b) accurate and complete copies in human readable and electronic form, 11.10(c) protection and ready retrieval, 11.10(d) limiting access to authorized individuals, 11.10(e) secure computer-generated time-stamped audit trails where "record changes shall not obscure previously recorded information", 11.10(g) authority checks, 11.50 signature manifestations, 11.70 signature-to-record linking.

Note that ISO 9001 has no explicit software-validation clause. For a plain 9001 shop, the obligation is control of documented information, not a validation protocol. Scope your effort accordingly.

2. Data-integrity controls that exist

2.1 Tamper-evident, append-only calibration ledger

Every calibration event is written to a ledger. Once an entry is committed (that is, once it leaves DRAFT), it cannot be edited or deleted.

How the tamper-evidence works. Each committed entry stores a `record_hash`: a SHA-256 digest over a canonical, key-sorted JSON serialization of that entry's fields, which includes the previous entry's `record_hash` as `prev_hash`. Entries are chained per workspace in insertion order, with `created_at` forced strictly monotonic so the ordering is a deterministic replay. Any alteration, insertion, or removal of a record changes its hash and breaks the chain from that point forward, and the break is detectable.

The hashed fields include: asset, event type, performed-at timestamp, performing user, calibration result, nominal value, tolerance, as-found and as-left readings, temperature, humidity, reference standard, measurements, notes, attachment reference, certificate number, service provider, traceability reference, correction reason, and the metrology fields listed in section 1.

Evidence files are hashed by content, not just by pointer. The SHA-256 of the uploaded certificate or photo is computed server-side and folded into the record hash. Swapping the file behind an unchanged link breaks the chain.

The immutability is enforced by the database, not by application code. A PostgreSQL trigger on the ledger table blocks, at the database level: deleting a committed entry, reverting a committed entry to DRAFT, and modifying any hashed or identity column of a committed entry. This means a direct SQL session against the production database cannot silently rewrite a calibration record. That is a stronger control than an application-layer check, and it is the specific point worth demonstrating to an assessor.

Change is represented by appending, never by overwriting. This is the direct answer to Part 11's requirement that record changes not obscure previously recorded information.

- A **correction** is a new appended entry that references the entry it supersedes and carries a free-text correction reason. The reason is mandatory (the API rejects a correction without one) and is itself part of the hash. The superseded entry stays in history, readable in full.
- A **void** is an appended tombstone event. The voided original stays in history badged as voided, and the instrument falls back to its prior calibration or to not-calibrated. A void can never be counted as a calibration.

One-click verification. Any authenticated user in the workspace can run a full chain verification, which walks every committed entry, recomputes each hash, checks continuity, and reports either a clean result with the count of entries verified or the first mismatched entry with its instrument tag. The result and the verifying user are recorded.

Independent verification off-platform. The audit export includes the `record_hash` and `prev_hash` values in the manifest CSV, plus a README with a step-by-step procedure to verify the chain **linkage** offline without Axiospec: every row's `prev_hash_hex` must equal the `record_hash_hex` of the row before it, so any removed, inserted, or reordered record shows up as a broken link. Be precise about the boundary. The manifest does not carry every field that feeds the hash function, so recomputing a record hash from the

CSV alone is not possible. Recomputation of an individual record hash happens server-side, in the app and at export time. Linkage is what you can prove yourself, without us, forever.

2.2 Audit trail

Calibration records. Each entry stores the performing user's id plus a frozen snapshot of their name, the performed-at timestamp, and the server-side created-at timestamp. When the entry goes through review it also stores the reviewer's id and name snapshot, the review timestamp, review notes, and any rejection reason. Prior values are preserved by construction: nothing is overwritten, so the "previous value" is the superseded entry, still readable.

Workspace administration. A separate activity log records team and configuration actions with the acting user, the target, a JSON record of what changed, the source IP, and a timestamp. Covered actions include user invites and revocations, role changes, user archival, email changes, API key issue and revoke, SSO configuration changes and SSO logins, webhook subscription changes, and billing trial start. It is readable in-app by workspace administrators, scoped hard to the workspace from the authenticated session rather than from a request parameter.

Known gap, disclosed. Changes to an instrument's master record (for example its calibration interval) are not currently captured in the system audit log. Calibration events themselves are immutable and fully attributed. The same applies to an instrument's tag, serial number, and location. If your procedure needs "who changed this instrument's interval and when", you must cover it with your own control until this is closed. See section 6.

2.3 Approvals (maker and checker)

Two-person review is available per instrument or workspace-wide. It is **opt-in and off by default.**

When review is required, the system refuses to let the submitter approve their own record. The check is unconditional at the top of both the approve and the reject path, and it also fails closed if the approver's identity cannot be resolved. Approving requires a manager or administrator role, checked both organization-wide and at the specific site the instrument belongs to, so an organization-wide manager who has been downgraded at that site is denied there. The generic record-update route refuses to set an approved or rejected status, so the workflow cannot be bypassed. Voids follow the same workflow, and a pending or rejected void does not hide the original.

When review is **not** required, the submission is auto-approved and the submitter is recorded as the approver. One person records and the record is immediately effective. State that plainly in your own risk assessment, and turn review on for the instruments where your risk assessment requires it.

2.4 Electronic signatures

What is real and shipping. Electronic signature is a per-workspace setting. It is optional, not mandatory. When a workspace enables it, approval requires the approver's own account password to be re-verified at the moment of signing, server-side against the stored password hash, before the approval proceeds. A wrong password is always refused with a 403, regardless of any configuration flag. The mobile app requires password entry when a calibration is recorded. Passwords are stored as PBKDF2-HMAC-SHA256 with 260,000 iterations and a 16-byte random salt per password, and verification is constant-time. A standalone

re-authentication endpoint exists for the same purpose. The approving user and the approval timestamp are recorded on the immutable ledger record, frozen by the database trigger described in section 2.1.

Two limits you must know before you rely on this.

1. **It is optional per workspace and not hard-enforced today.** If the client submits no signature password at all, the approval currently succeeds and logs a warning, rather than being refused. Only a wrong password is refused. The hard-enforcement switch exists in the code but is not enabled in the production environment.
2. **There is no stored cryptographic signature binding.** Do not expect a separate, retrievable signature artifact on the calibration record, and do not expect a signed flag in the API. The durable evidence is the approval record itself: approver identity, approver name snapshot, approval timestamp, and review notes, all of which are frozen by the immutability trigger.

Consequently Axiospec does **not** meet 21 CFR 11.50 and 11.70 today, and the two-distinct-identification-components expectation for non-continuous sessions cannot be met because there is no multi-factor authentication in the product. If Part 11 electronic signatures are a hard requirement for you, treat this as a gap and raise it with us before you buy.

2.5 Role-based access control

Five roles: super administrator, administrator, manager, technician, auditor. Enforcement is **server-side** on every route through FastAPI dependencies. The user's role is re-resolved from the database at request time rather than trusted from the session token, so a stale token cannot carry elevated privilege. Client-side gating exists but is cosmetic; the server is the enforcement point.

Relevant behaviors for 11.10(d) and (g) and for ISO/IEC 17025 7.11.3:

- Role-change authority is bounded. A manager can only manage technicians. Invite permissions are constrained by role.
- **The auditor role is enforced read-only globally.** All write HTTP methods are blocked for auditors, with exactly two allowlisted exceptions: requesting an audit-trail export, and revoking their own calendar feed token (which removes access and never grants any). This is the role to give your registrar or an external assessor.
- A **per-site access boundary** layers on top of role. A user can hold an organization-wide role and still be denied at a specific site, and this is checked on calibration submit, void, and approve.
- Only managers and administrators can void a calibration. Technicians may correct only their own records; managers and administrators may correct any.

Records are stored with row-level workspace scoping enforced in the data-access layer, with the workspace taken from a signature-verified session claim, never from a client-supplied header. Note the honest characterization: this is **application-enforced** workspace scoping, not PostgreSQL row-level security and not a separate database per customer. The ledger immutability, by contrast, is database-enforced.

3. What you should verify in your own environment

The following is a suggested protocol you execute and record. Nothing here has been executed for you. For each step, record the date, the person who executed it, the expected result, the actual result, pass or fail, and attach a screenshot. Under ISO/IEC 17025 7.11.2 this is the functional verification that belongs to you.

Installation qualification (IQ), configuration recorded

#	Check	Record
IQ-1	Workspace name, application URL, and date of first production use	
IQ-2	Named users, their roles, and their site grants	
IQ-3	Workspace settings recorded: approvals required yes/no, electronic signature setting on/off, enabled modules, custom fields defined	
IQ-4	Sites and locations configured, matching your facility list	
IQ-5	Instrument register loaded, count reconciled against your source register	
IQ-6	Supplier qualification record for CaliTech LLC opened, with this document attached	
IQ-7	Your controlled SOP naming Axiospec as the calibration record system issued and approved under your document control	

Operational qualification (OQ), functional testing

#	Test	Expected result
OQ-1	Record a calibration on a test instrument	Entry appears in that instrument's history with your name, the performed date, and the recorded readings
OQ-2	Attempt to edit that committed record	System refuses and directs you to issue a correction
OQ-3	Attempt to delete that committed record	System refuses, stating the ledger is append-only
OQ-4	Issue a correction without a reason, then with a reason	Refused without a reason; accepted with one; the original entry remains visible in history
OQ-5	As a manager, void a calibration	Original stays in history badged voided; instrument status falls back to the prior calibration or to not-calibrated
OQ-6	As a technician, attempt to void a calibration	Refused

#	Test	Expected result
OQ-7	Turn on approval for one instrument. Submit a calibration as user A, then attempt to approve it as user A	Refused, citing maker and checker separation
OQ-8	Approve it as user B	Approver name and approval timestamp are recorded on the entry and visible in history
OQ-9	Log in as an auditor-role user and attempt any change	All writes refused
OQ-10	Assign a user to Site 1 only, then attempt to act on an instrument at Site 2	Refused
OQ-11	Run chain verification from the audit area	Reports verified, with the count of entries verified. Record the date, the count, and the verifying user
OQ-12	Generate an unscoped audit export	ZIP downloads containing audit_manifest.csv, audit_summary.pdf, the README verification guide, and the attachment files
OQ-13	Follow the README procedure to verify chain linkage offline	Every row's `prev_hash_hex` equals the `record_hash_hex` of the row before it
OQ-14	Record an out-of-tolerance result	Instrument is flagged; the out-of-tolerance impact assessment can be recorded once and then locks
OQ-15	Confirm calibration status and next-due date display correctly for a known instrument (ISO/IEC 17025 6.4.8)	Status and due date match your expectation
OQ-16	Change a user's role, then open the workspace activity log	The change appears with the acting user, target, and timestamp
OQ-17	Edit an instrument's calibration interval, then check the activity log	**No entry appears. This is the known gap in section 2.2.** Record it as a control gap and document your compensating control
OQ-18	Print or export a calibration certificate for an approved record, then attempt the same for a voided record	Certificate is produced for the approved record; refused for the voided one

Performance qualification (PQ), your process with your people

#	Activity
PQ-1	Define the period (a full calibration cycle is preferable, one month is a common minimum)
PQ-2	Run in parallel with your existing register for that period. Reconcile instrument counts and due dates at the end

#	Activity
PQ-3	Confirm due and overdue notifications reach the right people on the expected schedule
PQ-4	Confirm your technicians can complete a calibration record per your SOP without workarounds
PQ-5	Run a mock audit. Pick one instrument at random and produce: full history, traceability reference, the reference standard used, evidence attachments, and proof the record has not been altered
PQ-6	Handle one real out-of-tolerance event end to end, including the impact assessment on prior measurements (ISO 9001 7.1.5.2)
PQ-7	Verify the contingency path in your SOP for when the system is unavailable
PQ-8	Write and approve the validation summary report. Sign it

Re-qualification. Define your trigger for re-testing. A practical rule for a Category 4 SaaS: re-execute the OQ subset that touches any function you rely on, whenever you materially change your configuration (approval settings, roles, sites, custom fields, standards tailoring), and on a periodic review interval you define. See section 5 for how vendor-side change works.

4. Record retention and export

Export is self-serve, complete, and not gated behind a paid tier or a support ticket. Managers, administrators, and auditors can generate it. Technicians retain per-instrument history in the app but not the whole-workspace export.

The export is a single ZIP containing:

- `audit_manifest.csv`: one row per instrument record, then one row per committed calibration event. Roughly 45 columns including instrument identity, site and location, all calibration fields, the metrology fields, approval and reviewer fields, out-of-tolerance impact, workspace custom fields as JSON, and the `record_hash_hex` and `prev_hash_hex` values. The hash columns are deliberately excluded from the CSV formula-injection guard so they are byte-exact for linkage comparison.
- `audit_summary.pdf`: a human-readable report with a compliance dashboard, a tamper-evident integrity verification section stating the chain verdict, the entries-verified count, the hash algorithm, and the genesis and head record hashes, then the calibration audit trail, the instrument roster, and out-of-tolerance detail. The exception table lists the 20 most recent qualifying events; the complete set is in `audit_manifest.csv`.
- `assets/<tag>/...`: the evidence files themselves, in their original format, grouped by instrument tag.
- A README verification guide with the export scope, coverage counts, the hash-chain explanation, and the offline linkage-verification procedure.

The archive is intended to support your 11.10(b) determination: it provides records in both human-readable (PDF) and electronic (CSV) form. Whether it satisfies 11.10(b) for your records is your determination. It is also the practical answer to vendor-continuity questions: the pack is self-contained, open-format, and its chain linkage is checkable without us.

Scoping and one important limit. Exports can be scoped by site, location, specific instruments, date range, and status, and the scope always intersects with the requester's own site permissions so it can only narrow. **A scoped or date-ranged export re-verifies each exported record's own hash but does not assert cross-record chain continuity, because a filtered set is a deliberate subset of the chain.** Only an unscoped, all-history export gets the full chain walk. Use an unscoped export when you need the continuity proof. The README states this too.

Retention while the account is active: records are retained for the life of the workspace. No individual committed calibration record can be edited or deleted by anyone, including us.

Retention after closure: when an account is closed, data is retained for **730 days (about 24 months)** so you can sign back in and export. Billing is cancelled immediately at the request, so nothing bills during that window. After the window, a hard purge deletes the workspace's data across every table and removes the stored evidence files. That purge is the **only** sanctioned path by which committed ledger rows are ever removed, and it is a whole-workspace operation, never a per-record delete.

Backups: the production database has automated daily backups with a 14-day retention window, deletion protection enabled, and a final snapshot on any instance teardown. See section 6 for what we do not claim about recovery.

Hosting: production runs on Amazon Web Services in us-east-1, United States. The database is encrypted at rest and has no public internet access. The application and API are served only over HTTPS with TLS 1.2 minimum. Account-wide AWS CloudTrail is enabled with log-file integrity validation and a 365-day retention window. A separate security overview is published at axiospec.com/security.

5. Change management

How changes are made and gated.

- Production deployments are **manual-trigger only**. There is no automatic push to production.
- A production deployment is blocked unless three jobs pass first: the full backend test suite, an OpenAPI schema validation job, and a dependency vulnerability audit. A red test suite stops the deployment.
- The backend test suite is **2,465 test functions across 197 test files**. There are a further 233 test files on the web front end. These are automated regression tests that run on every change.
- Every production build is published under an immutable per-commit image tag, so there is a defined rollback target for each release.
- Staging and production are separate environments with separate infrastructure. Changes reach staging first.

Be clear about what this is and is not. An automated test suite of that size is a genuine and citable software development control, and it is good raw material for an operational-qualification argument. It is **not** a validation package. It is not written against a formal functional specification, there is no requirement-to-

test traceability matrix, and there is no signed release record. A computer-system-validation reviewer will not accept it as one, and we will not present it as one.

How you know when something changes.

Axiospec is multi-tenant software as a service. All customers run one production version. **You cannot pin a version, defer an update, or run a prior release.** That is a real constraint for a validated environment and you should record it in your risk assessment.

Today there is **no published changelog, no release-notes page, and no written change-notification commitment.** If your procedure requires advance notice of changes to a validated system, ask us for that commitment in writing before you buy, at support@axiospec.com. We would rather tell you it does not exist than let you discover it during an audit.

What we suggest you do about it, given the above: define a periodic re-verification interval in your SOP (for example, re-run the OQ subset quarterly and after any change you notice to a function you rely on), and re-run chain verification and record the result on that same interval. Chain verification takes one click and produces a dated, attributable result.

6. Limits of what this software does

Stated plainly, because a small vendor that names its limits is easier to qualify than one that dodges.

Certifications and assessments we do not hold. No SOC 2, Type I or Type II. No ISO/IEC 27001. No third-party penetration test. No HIPAA business associate agreement, and we do not accept protected health information. No FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR, or DFARS 252.204-7012. If you handle controlled unclassified information or export-controlled data, Axiospec is not currently a fit. No published data processing addendum, no standard contractual clauses, and no EU data residency; all data is in the United States.

No vendor validation package. There is no IQ/OQ/PQ package, no validation protocol, no traceability matrix, and no validation summary report produced by us. Section 3 is a checklist for you to execute, not evidence that anything was executed.

No compliance claim. Axiospec does not certify, ensure, or guarantee your compliance with any standard. It supports and documents calibration records and keeps them audit-ready. Conformance is determined by your quality unit, your registrar, your accreditation body, or your inspector.

We do not claim conformance with 21 CFR Part 11. The record-integrity building blocks are genuinely strong: database-enforced immutability, a SHA-256 hash chain, attributed and timestamped entries, append-only corrections that do not obscure prior information, and two-person review. The signature controls are not there yet. See section 2.4: electronic signature is optional per workspace rather than mandatory, there is no stored signature binding on the record, there is no signature-meaning field, and there is no multi-factor identification. We publish a feature mapping with the gaps marked; we do not publish a compliance claim.

No multi-factor authentication. There is no built-in TOTP, authenticator app, WebAuthn, SMS, or backup codes. The only route to a second factor today is signing in through Google, where your own identity provider enforces it. Per-workspace enterprise SSO over OIDC and SAML is built and tested in the backend

but is not enabled on production and should be treated as available on request, not as a shipping feature. If your IT policy requires enforced MFA for all QMS systems, this is a hard blocker today. Ask us for the current status before you buy.

Asset master-record changes are not logged. Section 2.2 and test OQ-17. Calibration events are fully covered by the ledger. Changes to the instrument's descriptive record, including its calibration interval, are not attributed in the activity log.

Filtered exports do not prove chain continuity. Section 4. Use an unscoped export for that.

No availability commitment. There is no uptime SLA, no status page, and no published availability history. The production database is a single instance in a single availability zone, so an availability-zone failure requires a restore rather than a failover. We do not publish a recovery time or recovery point objective, and no restore drill has been documented. Backups are configured and retained for 14 days; that is a true statement about backups, not a proven statement about recovery. Your SOP should include a contingency for the system being unavailable, which ISO/IEC 17025 assessors ask about anyway.

No documented incident response plan or contractual breach-notification window. Infrastructure alarms are configured in CloudWatch and delivered to an on-call email address. That is monitoring, not an incident-response program.

No customer-managed encryption keys. Encryption uses AWS-managed keys.

Records can be deleted in exactly one way. No individual committed record can be edited or deleted by anyone. The only deletion path is a customer-requested full-workspace purge after the 730-day retention window.

We do not perform calibration. Axiospec is a record-keeping system, not an accredited calibration laboratory, and did not perform any measurement in your records.

How to use this document. Attach it to your supplier qualification record for CaliTech LLC (ISO 9001 clause 8.4, ISO/IEC 17025 clause 6.6). Reference it from your validation plan as the vendor functional and control description. Execute section 3 in your own workspace and retain the signed result as your qualification evidence. Record the section 6 limits in your risk assessment along with your compensating controls.

If a claim in this document does not match what you observe in the product, tell us at support@axiospec.com and we will correct the document.

Axiospec is published by CaliTech LLC, Knoxville, Tennessee. Axiospec supports and documents your calibration program and keeps it audit-ready. It does not certify, ensure, or guarantee compliance with any standard; that determination belongs to you and your assessor. Questions: support@axiospec.com