Zusammenfassung der Softwarevalidierung

Axiospec Kalibriermanagement Erstellt für den Qualitätsmanager, den Validierungsverantwortlichen oder den IT-Prüfer, der Axiospec als maßgebliches System für Kalibrieraufzeichnungen bewertet.

Dokumentversion 1.0. Zuletzt überprüft am 19.08.2026. Herausgegeben von CaliTech LLC, Knoxville, Tennessee (USA). Fragen: support@axiospec.com, Antwort innerhalb eines Werktags.

Lesen Sie dies zuerst

Dieses Dokument ist **ein Beitrag zu Ihrer Validierungsdokumentation. Es ist keine Validierungsdokumentation.**

Axiospec validiert Ihre Instanz nicht, zertifiziert Ihre Konformität nicht und führt Ihre Qualifizierung nicht durch. Die Validierung ist eine Feststellung, die Sie über Ihren eigenen Verwendungszweck, Ihre Konfiguration, Ihre Verfahren und Ihr Personal treffen. Ob Sie sie erfüllt haben, entscheidet Ihre Zertifizierungsstelle, Ihr Begutachter oder Ihr Inspektor.

Was Ihnen dieses Dokument bietet: eine Erklärung zum Verwendungszweck, eine Beschreibung der im Produkt vorhandenen Kontrollen zur Datenintegrität und wie sie erzwungen werden, eine Checkliste, die Sie in Ihrem eigenen Arbeitsbereich durchführen und unterschreiben können, unsere Praxis im Änderungsmanagement und eine klare Liste dessen, was die Software nicht leistet.

Nach der Kategorisierung von GAMP 5 wird ein konfiguriertes, mandantenfähiges SaaS-Verzeichnis dieser Art üblicherweise als Kategorie 4 (konfiguriertes Produkt) behandelt. Das bedeutet, dass Ihr Validierungsaufwand risikobasiert ist und sich auf die Dokumentation des Anbieters sowie auf Ihre eigenen Konfigurations- und Prozesstests stützt. Bestätigen Sie diese Kategorisierung anhand Ihres eigenen Verfahrens.

1. Erklärung zum Verwendungszweck

Axiospec ist ein Dokumentationssystem für Mess- und Prüfmittel. Sein Verwendungszweck ist:

- Ein Verzeichnis der Messmittel führen, einschließlich Identifikation, Hersteller, Modell, Seriennummer, Ort, Standort und im Arbeitsbereich definierter benutzerdefinierter Felder.
- Kalibrier- und Prüfereignisse zu diesen Messmitteln erfassen, einschließlich der Messwerte vor der Justierung und nach der Justierung, Nennwert, Toleranz, Ergebnis, Umgebungsbedingungen, verwendetem Bezugsnormal, Kalibrierscheinnummer, Dienstleister und Rückführbarkeitsnachweis.
- Die in Abläufen nach ISO/IEC 17025 verwendeten messtechnischen Felder erfassen: Messunsicherheit, Erweiterungsfaktor, Vertrauensniveau, Entscheidungsregel, Konformitätsaussage und die Kalibrierscheinnummer des Bezugsnormals selbst.
- Den Kalibrierstatus jedes Messmittels und sein nächstes Fälligkeitsdatum ausweisen und überfällige sowie bald fällige Messmittel hervorheben.

- Diese Aufzeichnungen in einer Form aufbewahren, an die nur angehängt werden kann und die manipulationserkennbar ist, mit Zuordnung und Zeitstempeln.
- Kalibrieraufzeichnungen optional durch eine Freigabe im Vier-Augen-Prinzip leiten, bevor sie wirksam werden.
- Einen vollständigen, für Menschen und Maschinen lesbaren Export des Verzeichnisses und seiner Historie für Audits erzeugen.

Axiospec ist **kein** akkreditiertes Kalibrierlaboratorium und führt keine Messungen durch. Jedes Dokument, das das System erzeugt, trägt wörtlich diese Aussage:

> "Die Kalibrierdaten wurden von Personal des Arbeitsbereichs erfasst. Axiospec ist ein Dokumentationssystem, kein akkreditiertes Kalibrierlaboratorium, und hat diese Messung nicht durchgeführt."

Axiospec ist keine Medizinproduktesoftware, und ein Bezug zu IEC 62304 wird weder behauptet noch nahegelegt. IEC 62304 regelt Software, die ein Medizinprodukt ist oder Teil eines solchen. Ein Kalibrierverzeichnis ist ein Werkzeug des Qualitätsmanagementsystems.

Welche Abschnitte die Erwartungen an ein solches System bestimmen

Der Text der ISO-Normen ist urheberrechtlich geschützt, daher folgen hier Verweise auf Abschnitte mit sinngemäßer Wiedergabe, keine Zitate. Prüfen Sie sie anhand Ihres eigenen lizenzierten Exemplars.

- **ISO 9001:2015, Abschnitt 7.1.5.2** (messtechnische Rückführbarkeit): Messmittel, die in festgelegten Abständen gegen rückführbare Normale kalibriert oder verifiziert werden, deren Kalibrierstatus erkennbar ist, die vor Justierungen geschützt sind, die das Ergebnis ungültig machen würden, und eine Bewertung früherer Ergebnisse, wenn ein Messmittel als ungeeignet befunden wird.
- **ISO 9001:2015, Abschnitt 7.5.3** (Lenkung dokumentierter Information): Verfügbarkeit, Schutz vor Verlust der Integrität, Zugriffssteuerung, Ablage und Erhaltung, Überwachung von Änderungen und Versionen, Aufbewahrung und Verfügung über den weiteren Verbleib.
- **ISO 9001:2015, Abschnitt 8.4** und **ISO/IEC 17025:2017, Abschnitt 6.6** (extern bereitgestellte Produkte und Dienstleistungen): Sie müssen Ihre Qualifizierung von Axiospec als Lieferant bewerten und aufzeichnen. Dieses Dokument soll als Nachweis für diese Aufzeichnung dienen.
- **ISO/IEC 17025:2017, Abschnitt 6.4** (Einrichtungen), insbesondere 6.4.6 (Kalibrierung, wenn Genauigkeit oder Messunsicherheit die Gültigkeit beeinflussen), 6.4.8 (Kennzeichnung oder Codierung des Status, damit der Benutzer den Kalibrierstatus oder die Gültigkeitsdauer leicht erkennt) und 6.4.13 (der geforderte Inhalt der Aufzeichnungen zu Einrichtungen).
- **ISO/IEC 17025:2017, Abschnitt 7.11** (Lenkung der Daten und Informationsmanagement), insbesondere 7.11.2 (das Informationsmanagementsystem wird hinsichtlich seiner Funktionalität validiert, einschließlich der Schnittstellen) und 7.11.3 (geschützt vor unbefugtem Zugriff, gesichert gegen Manipulation und Verlust, gemäß Spezifikation betrieben, so gepflegt, dass die Datenintegrität gewahrt bleibt, mit Aufzeichnung von Ausfällen und Korrekturmaßnahmen).
- **ISO 13485:2016, Abschnitt 4.1.6**: Verfahren zur Validierung von Computersoftware, die im QM-System eingesetzt wird, vor der ersten Anwendung und nach Änderungen, mit einem risikoangemessenen Ansatz

und mit geführten Aufzeichnungen.

- **21 CFR Part 11**, wenn die Kalibrieraufzeichnungen Ihre regulierten maßgeblichen Aufzeichnungen sind: 11.10(a) Validierung, 11.10(b) genaue und vollständige Kopien in für Menschen lesbarer und elektronischer Form, 11.10(c) Schutz und schnelle Abrufbarkeit, 11.10(d) Beschränkung des Zugriffs auf befugte Personen, 11.10(e) sichere, computergenerierte Audit-Trails mit Zeitstempel, bei denen "Änderungen an Aufzeichnungen zuvor erfasste Informationen nicht verdecken dürfen", 11.10(g) Berechtigungsprüfungen, 11.50 Signaturkennzeichnung, 11.70 Verknüpfung von Signatur und Aufzeichnung.

Beachten Sie, dass ISO 9001 keinen ausdrücklichen Abschnitt zur Softwarevalidierung enthält. Für einen reinen 9001-Betrieb besteht die Pflicht in der Lenkung dokumentierter Information, nicht in einem Validierungsprotokoll. Bemessen Sie Ihren Aufwand entsprechend.

2. Vorhandene Kontrollen zur Datenintegrität

2.1 Manipulationserkennbares Kalibrierjournal, an das nur angehängt werden kann

Jedes Kalibriereereignis wird in ein Journal geschrieben. Sobald ein Eintrag festgeschrieben ist (also den Status Entwurf, DRAFT, verlassen hat), kann er weder bearbeitet noch gelöscht werden.

Wie die Manipulationserkennung funktioniert. Jeder festgeschriebene Eintrag speichert einen `record_hash`: einen SHA-256-Hashwert über eine kanonische JSON-Serialisierung der Felder dieses Eintrags mit sortierten Schlüsseln, die den `record_hash` des vorherigen Eintrags als `prev_hash` enthält. Die Einträge werden je Arbeitsbereich in Einfügereihenfolge verkettet, wobei `created_at` streng monoton steigend erzwungen wird, sodass die Reihenfolge eine deterministische Wiedergabe ist. Jede Änderung, Einfügung oder Entfernung eines Datensatzes ändert seinen Hash und unterbricht die Kette ab diesem Punkt, und die Unterbrechung ist erkennbar.

In den Hash fließen ein: Messmittel, Ereignistyp, Zeitstempel der Durchführung, durchführender Benutzer, Kalibrierergebnis, Nennwert, Toleranz, Messwerte vor der Justierung und nach der Justierung, Temperatur, Luftfeuchte, Bezugsnormal, Messungen, Notizen, Anhangsverweis, Kalibrierscheinnummer, Dienstleister, Rückführbarkeitsnachweis, Korrekturgrund und die in Abschnitt 1 genannten messtechnischen Felder.

Nachweisdateien fließen mit ihrem Inhalt in den Hash ein, nicht nur mit ihrem Verweis. Der SHA-256-Hash des hochgeladenen Kalibrierscheins oder Fotos wird serverseitig berechnet und in den Hash des Datensatzes eingerechnet. Wer die Datei hinter einem unveränderten Link austauscht, unterbricht die Kette.

Die Unveränderlichkeit erzwingt die Datenbank, nicht der Anwendungscode. Ein PostgreSQL-Trigger auf der Journaltabelle verhindert auf Datenbankebene: das Löschen eines festgeschriebenen Eintrags, das Zurücksetzen eines festgeschriebenen Eintrags auf Entwurf und die Änderung jeder gehashten oder identitätsbildenden Spalte eines festgeschriebenen Eintrags. Eine direkte SQL-Sitzung auf der Produktivdatenbank kann einen Kalibrierdatensatz also nicht unbemerkt umschreiben. Das ist eine stärkere Kontrolle als eine Prüfung in der Anwendungsschicht, und genau diesen Punkt lohnt es sich einem Begutachter vorzuführen.

Änderungen werden durch Anhängen abgebildet, nie durch Überschreiben. Das ist die direkte Antwort auf die Forderung von Part 11, dass Änderungen an Aufzeichnungen zuvor erfasste Informationen nicht verdecken dürfen.

- Eine **Korrektur** ist ein neu angehängter Eintrag, der auf den ersetzten Eintrag verweist und einen Korrekturgrund als Freitext trägt. Der Grund ist Pflicht (die API weist eine Korrektur ohne Grund zurück) und ist selbst Teil des Hashes. Der ersetzte Eintrag bleibt vollständig lesbar in der Historie.
- Eine **Stornierung** ist ein angehängtes Stornoereignis. Das stornierte Original bleibt mit dem Kennzeichen storniert in der Historie, und das Messmittel fällt auf seine vorherige Kalibrierung oder auf nicht kalibriert zurück. Eine Stornierung kann nie als Kalibrierung zählen.

Prüfung mit einem Klick. Jeder angemeldete Benutzer im Arbeitsbereich kann eine vollständige Kettenprüfung starten, die jeden festgeschriebenen Eintrag durchläuft, jeden Hash neu berechnet, die Kontinuität prüft und entweder ein sauberes Ergebnis mit der Anzahl der geprüften Einträge meldet oder den ersten abweichenden Eintrag mit seiner Messmittelkennung. Ergebnis und prüfender Benutzer werden aufgezeichnet.

Unabhängige Prüfung außerhalb der Plattform. Der Auditexport enthält die Werte `record_hash` und `prev_hash` in der Manifest-CSV sowie eine README mit einem Schritt-für-Schritt-Verfahren, um die **Verkettung** offline ohne Axiospec zu prüfen: Der `prev_hash_hex` jeder Zeile muss dem `record_hash_hex` der vorherigen Zeile entsprechen, sodass jeder entfernte, eingefügte oder umsortierte Datensatz als unterbrochene Verknüpfung auffällt. Die Grenze sollte man genau benennen. Das Manifest enthält nicht jedes Feld, das in die Hash-Funktion einfließt, daher lässt sich ein Datensatz-Hash nicht allein aus der CSV neu berechnen. Die Neuberechnung eines einzelnen Datensatz-Hashes erfolgt serverseitig, in der Anwendung und beim Export. Die Verkettung ist das, was Sie selbst nachweisen können, ohne uns, für immer.

2.2 Audit-Trail

Kalibrieraufzeichnungen. Jeder Eintrag speichert die ID des durchführenden Benutzers und eine eingefrorene Momentaufnahme seines Namens, den Zeitstempel der Durchführung und den serverseitigen Erstellungszeitstempel. Durchläuft der Eintrag eine Prüfung, speichert er außerdem die ID und die Namensmomentaufnahme des Prüfers, den Prüfzeitstempel, die Prüfnotizen und einen etwaigen Ablehnungsgrund. Frühere Werte bleiben konstruktionsbedingt erhalten: Nichts wird überschrieben, der "vorherige Wert" ist also der ersetzte Eintrag, der weiterhin lesbar ist.

Verwaltung des Arbeitsbereichs. Ein separates Aktivitätsprotokoll zeichnet Team- und Konfigurationsaktionen auf, mit handelndem Benutzer, Ziel, einem JSON-Datensatz der Änderung, Quell-IP und Zeitstempel. Erfasst werden unter anderem Benutzereinladungen und Widerrufe, Rollenänderungen, das Archivieren von Benutzern, Änderungen der E-Mail-Adresse, das Ausstellen und Widerrufen von API-Schlüsseln, Änderungen der SSO-Konfiguration und SSO-Anmeldungen, Änderungen an Webhook-Abonnements sowie der Start einer Testphase in der Abrechnung. Administratoren des Arbeitsbereichs können es in der Anwendung lesen, streng auf den Arbeitsbereich der angemeldeten Sitzung begrenzt und nicht auf einen Anfrageparameter.

Bekannte Lücke, offengelegt. Änderungen am Stammdatensatz eines Messmittels (zum Beispiel an seinem Kalibrierintervall) werden derzeit nicht im Audit-Log des Systems erfasst. Die Kalibrierereignisse selbst sind unveränderlich und vollständig zugeordnet. Dasselbe gilt für Kennung, Seriennummer und Ort eines Messmittels. Wenn Ihr Verfahren wissen muss, "wer das Intervall dieses Messmittels wann geändert

hat", müssen Sie das mit einer eigenen Kontrolle abdecken, bis diese Lücke geschlossen ist. Siehe Abschnitt 6.

2.3 Freigaben (Vier-Augen-Prinzip)

Die Prüfung durch zwei Personen ist je Messmittel oder für den ganzen Arbeitsbereich verfügbar. Sie ist **optional und standardmäßig deaktiviert.**

Ist eine Prüfung erforderlich, lässt das System nicht zu, dass die einreichende Person ihren eigenen Datensatz freigibt. Die Prüfung erfolgt bedingungslos gleich zu Beginn sowohl des Freigabe- als auch des Ablehnungspfads und schlägt auch dann sicher fehl, wenn sich die Identität der freigebenden Person nicht auflösen lässt. Die Freigabe erfordert die Rolle Manager oder Administrator, geprüft sowohl organisationsweit als auch am konkreten Standort, zu dem das Messmittel gehört, sodass ein organisationsweiter Manager, der an diesem Standort herabgestuft wurde, dort abgewiesen wird. Die allgemeine Route zum Aktualisieren von Datensätzen verweigert das Setzen eines Status freigegeben oder abgelehnt, sodass der Workflow nicht umgangen werden kann. Stornierungen folgen demselben Workflow, und eine ausstehende oder abgelehnte Stornierung verdeckt das Original nicht.

Ist **keine** Prüfung erforderlich, wird die Einreichung automatisch freigegeben, und die einreichende Person wird als Freigebende erfasst. Eine Person erfasst, und der Datensatz ist sofort wirksam. Halten Sie das in Ihrer eigenen Risikobewertung klar fest und aktivieren Sie die Prüfung für die Messmittel, bei denen Ihre Risikobewertung es verlangt.

2.4 Elektronische Signaturen

Was real und verfügbar ist. Die elektronische Signatur ist eine Einstellung je Arbeitsbereich. Sie ist optional, nicht verpflichtend. Aktiviert ein Arbeitsbereich sie, verlangt die Freigabe, dass das Passwort des eigenen Kontos der freigebenden Person im Moment der Signatur erneut geprüft wird, serverseitig gegen den gespeicherten Passwort-Hash, bevor die Freigabe fortgesetzt wird. Ein falsches Passwort wird immer mit einem 403 abgewiesen, unabhängig von jedem Konfigurationsschalter. Die mobile App verlangt bei der Erfassung einer Kalibrierung das Passwort. Passwörter werden als PBKDF2-HMAC-SHA256 mit 260.000 Iterationen und einem zufälligen 16-Byte-Salt je Passwort gespeichert, und die Prüfung erfolgt in konstanter Zeit. Für denselben Zweck gibt es einen eigenständigen Endpunkt zur erneuten Authentifizierung. Der freigebende Benutzer und der Freigabezeitstempel werden im unveränderlichen Journaleintrag erfasst und durch den in Abschnitt 2.1 beschriebenen Datenbank-Trigger eingefroren.

Zwei Grenzen, die Sie kennen müssen, bevor Sie sich darauf verlassen.

1. **Sie ist je Arbeitsbereich optional und wird heute nicht strikt erzwungen.** Sendet der Client überhaupt kein Signaturpasswort, wird die Freigabe derzeit durchgeführt und eine Warnung protokolliert, statt sie abzuweisen. Nur ein falsches Passwort wird abgewiesen. Der Schalter für die strikte Erzwingung existiert im Code, ist in der Produktivumgebung aber nicht aktiviert.
2. **Es gibt keine gespeicherte kryptografische Signaturbindung.** Erwarten Sie kein separates, abrufbares Signaturartefakt am Kalibrierdatensatz und kein Kennzeichen "signiert" in der API. Der dauerhafte Nachweis ist der Freigabedatensatz selbst: Identität der freigebenden Person, Momentaufnahme ihres Namens, Freigabezeitstempel und Prüfnotizen, alles durch den Unveränderlichkeits-Trigger eingefroren.

Folglich erfüllt Axiospec 21 CFR 11.50 und 11.70 heute **nicht**, und die Erwartung zweier unterschiedlicher Identifikationskomponenten für nicht zusammenhängende Sitzungen kann nicht erfüllt werden, weil es im Produkt keine Multi-Faktor-Authentifizierung gibt. Wenn elektronische Signaturen nach Part 11 für Sie eine harte Anforderung sind, behandeln Sie das als Lücke und sprechen Sie uns vor dem Kauf darauf an.

2.5 Rollenbasierte Zugriffssteuerung

Fünf Rollen: Super-Administrator, Administrator, Manager, Techniker, Auditor. Die Erzwingung erfolgt **serverseitig** auf jeder Route über FastAPI-Abhängigkeiten. Die Rolle des Benutzers wird zum Zeitpunkt der Anfrage erneut aus der Datenbank ermittelt, statt dem Sitzungstoken zu vertrauen, sodass ein veralteter Token keine erhöhten Rechte mitführen kann. Clientseitige Einschränkungen gibt es auch, sie sind aber kosmetisch; der Server ist der Ort der Erzwingung.

Relevante Verhaltensweisen für 11.10(d) und (g) sowie für ISO/IEC 17025 7.11.3:

- Die Befugnis zu Rollenänderungen ist begrenzt. Ein Manager kann nur Techniker verwalten. Einladungsrechte sind nach Rolle eingeschränkt.
- **Die Auditor-Rolle ist systemweit schreibgeschützt.** Alle schreibenden HTTP-Methoden sind für Auditoren gesperrt, mit genau zwei zugelassenen Ausnahmen: das Anfordern eines Exports des Audit-Trails und das Widerrufen des eigenen Kalender-Feed-Tokens (was einen Zugriff entfernt und nie einen gewährt). Das ist die Rolle, die Sie Ihrer Zertifizierungsstelle oder einem externen Begutachter geben.
- Über der Rolle liegt eine **Zugriffsgrenze je Standort**. Ein Benutzer kann eine organisationsweite Rolle haben und an einem bestimmten Standort trotzdem abgewiesen werden, und das wird beim Einreichen, Stornieren und Freigeben von Kalibrierungen geprüft.
- Nur Manager und Administratoren können eine Kalibrierung stornieren. Techniker dürfen nur ihre eigenen Datensätze korrigieren; Manager und Administratoren dürfen jeden korrigieren.

Die Datensätze werden mit einer zeilenbasierten Abgrenzung je Arbeitsbereich gespeichert, die in der Datenzugriffsschicht erzwungen wird, wobei der Arbeitsbereich aus einem Claim einer signaturgeprüften Sitzung stammt, nie aus einem vom Client gelieferten Header. Beachten Sie die ehrliche Einordnung: Das ist eine **von der Anwendung erzwungene** Abgrenzung je Arbeitsbereich, keine Sicherheit auf Zeilenebene von PostgreSQL und keine eigene Datenbank je Kunde. Die Unveränderlichkeit des Journals wird dagegen von der Datenbank erzwungen.

3. Was Sie in Ihrer eigenen Umgebung prüfen sollten

Das Folgende ist ein vorgeschlagenes Protokoll, das Sie durchführen und aufzeichnen. Nichts davon wurde für Sie durchgeführt. Halten Sie für jeden Schritt Datum, ausführende Person, erwartetes Ergebnis, tatsächliches Ergebnis und Bestanden oder Nicht bestanden fest und fügen Sie einen Screenshot bei. Nach ISO/IEC 17025 7.11.2 ist das die Funktionsprüfung, die bei Ihnen liegt.

Installationsqualifizierung (IQ), Konfiguration aufgezeichnet

Nr.	Prüfung	Aufzeichnung
IQ-1	Name des Arbeitsbereichs, URL der Anwendung und Datum der ersten produktiven Nutzung	

Nr.	Prüfung	Aufzeichnung
IQ-2	Namentlich benannte Benutzer, ihre Rollen und ihre Standortberechtigungen	
IQ-3	Einstellungen des Arbeitsbereichs aufgezeichnet: Freigaben erforderlich ja/nein, elektronische Signatur an/aus, aktivierte Module, definierte benutzerdefinierte Felder	
IQ-4	Standorte und Orte konfiguriert, passend zu Ihrer Liste der Einrichtungen	
IQ-5	Messmittelverzeichnis geladen, Anzahl mit Ihrem Quellverzeichnis abgeglichen	
IQ-6	Lieferantenqualifizierung für CaliTech LLC angelegt, mit diesem Dokument als Anlage	
IQ-7	Ihre gelenkte Verfahrensanweisung, die Axiospec als System für Kalibrieraufzeichnungen benennt, im Rahmen Ihrer Dokumentenlenkung herausgegeben und freigegeben	

Funktionsqualifizierung (OQ), Funktionstests

Nr.	Test	Erwartetes Ergebnis
OQ-1	Eine Kalibrierung für ein Testmessmittel erfassen	Der Eintrag erscheint in der Historie dieses Messmittels mit Ihrem Namen, dem Durchführungsdatum und den erfassten Messwerten
OQ-2	Versuchen, diesen festgeschriebenen Datensatz zu bearbeiten	Das System lehnt ab und verweist Sie auf eine Korrektur
OQ-3	Versuchen, diesen festgeschriebenen Datensatz zu löschen	Das System lehnt ab und nennt das Journal nur anhängbar
OQ-4	Eine Korrektur ohne Begründung und danach mit Begründung erstellen	Ohne Begründung abgelehnt; mit Begründung angenommen; der ursprüngliche Eintrag bleibt in der Historie sichtbar
OQ-5	Als Manager eine Kalibrierung stornieren	Das Original bleibt mit dem Kennzeichen storniert in der Historie; der Status des Messmittels fällt auf die vorherige Kalibrierung oder auf nicht kalibriert zurück
OQ-6	Als Techniker versuchen, eine Kalibrierung zu stornieren	Abgelehnt
OQ-7	Die Freigabe für ein Messmittel aktivieren. Eine Kalibrierung als Benutzer A einreichen und dann versuchen, sie als Benutzer A freizugeben	Abgelehnt, mit Verweis auf das Vier-Augen-Prinzip
OQ-8	Sie als Benutzer B freigeben	Name der freigebenden Person und Freigabezeitstempel werden am Eintrag erfasst und sind in der Historie sichtbar

Nr.	Test	Erwartetes Ergebnis
OQ-9	Als Benutzer mit Auditor-Rolle anmelden und eine beliebige Änderung versuchen	Alle Schreibzugriffe abgelehnt
OQ-10	Einen Benutzer nur Standort 1 zuweisen und dann versuchen, bei einem Messmittel an Standort 2 zu handeln	Abgelehnt
OQ-11	Die Kettenprüfung im Auditbereich ausführen	Meldet geprüft, mit der Anzahl der geprüften Einträge. Datum, Anzahl und prüfenden Benutzer aufzeichnen
OQ-12	Einen Auditexport ohne Umfang erzeugen	Eine ZIP-Datei wird heruntergeladen, die audit_manifest.csv, audit_summary.pdf, den README-Prüfleitfaden und die Anhangsdateien enthält
OQ-13	Dem README-Verfahren folgen, um die Verkettung offline zu prüfen	Der `prev_hash_hex` jeder Zeile entspricht dem `record_hash_hex` der vorherigen Zeile
OQ-14	Ein Ergebnis außerhalb der Toleranz erfassen	Das Messmittel wird markiert; die Bewertung der Auswirkung der Toleranzüberschreitung kann einmal erfasst werden und wird danach gesperrt
OQ-15	Bestätigen, dass Kalibrierstatus und nächstes Fälligkeitsdatum für ein bekanntes Messmittel korrekt angezeigt werden (ISO/IEC 17025 6.4.8)	Status und Fälligkeitsdatum entsprechen Ihrer Erwartung
OQ-16	Die Rolle eines Benutzers ändern und dann das Aktivitätsprotokoll des Arbeitsbereichs öffnen	Die Änderung erscheint mit handelndem Benutzer, Ziel und Zeitstempel
OQ-17	Das Kalibrierintervall eines Messmittels bearbeiten und dann das Aktivitätsprotokoll prüfen	**Es erscheint kein Eintrag. Das ist die bekannte Lücke aus Abschnitt 2.2.** Als Kontrolllücke aufzeichnen und Ihre ausgleichende Kontrolle dokumentieren
OQ-18	Einen Kalibrierschein für einen freigegebenen Datensatz drucken oder exportieren und dann dasselbe für einen stornierten Datensatz versuchen	Für den freigegebenen Datensatz wird der Kalibrierschein erzeugt; für den stornierten wird er abgelehnt

Leistungsqualifizierung (PQ), Ihr Prozess mit Ihrem Personal

Nr.	Tätigkeit
PQ-1	Den Zeitraum festlegen (ein vollständiger Kalibrierzyklus ist vorzuziehen, ein Monat ist ein übliches Minimum)
PQ-2	In diesem Zeitraum parallel zu Ihrem bestehenden Verzeichnis arbeiten. Am Ende Messmittelanzahl und Fälligkeitsdaten abgleichen
PQ-3	Bestätigen, dass Fälligkeits- und Überfälligkeitshinweise die richtigen Personen im erwarteten Rhythmus erreichen

Nr.	Tätigkeit
PQ-4	Bestätigen, dass Ihre Techniker eine Kalibrieraufzeichnung gemäß Ihrer Verfahrensanweisung ohne Umwege abschließen können
PQ-5	Ein Probeaudit durchführen. Ein Messmittel zufällig auswählen und vorlegen: vollständige Historie, Rückführbarkeitsnachweis, verwendetes Bezugsnormal, Nachweisanhänge und den Nachweis, dass der Datensatz nicht verändert wurde
PQ-6	Ein echtes Ereignis mit Toleranzüberschreitung von Anfang bis Ende bearbeiten, einschließlich der Bewertung der Auswirkung auf frühere Messungen (ISO 9001 7.1.5.2)
PQ-7	Den Notfallweg Ihrer Verfahrensanweisung für den Fall prüfen, dass das System nicht verfügbar ist
PQ-8	Den zusammenfassenden Validierungsbericht verfassen und freigeben. Unterschreiben

Requalifizierung. Legen Sie fest, was einen erneuten Test auslöst. Eine praktische Regel für ein SaaS der Kategorie 4: Führen Sie die OQ-Teilmenge, die eine Funktion betrifft, auf die Sie sich verlassen, erneut durch, wann immer Sie Ihre Konfiguration wesentlich ändern (Freigabeeinstellungen, Rollen, Standorte, benutzerdefinierte Felder, Anpassung an Normen), und in einem von Ihnen festgelegten regelmäßigen Überprüfungsintervall. Wie Änderungen auf Anbieterseite ablaufen, steht in Abschnitt 5.

4. Aufbewahrung und Export von Aufzeichnungen

Der Export ist Self-Service, vollständig und weder an einen kostenpflichtigen Tarif noch an einen Supportfall gebunden. Manager, Administratoren und Auditoren können ihn erzeugen. Techniker behalten die Historie je Messmittel in der Anwendung, aber nicht den Export des ganzen Arbeitsbereichs.

Der Export ist eine einzige ZIP-Datei mit:

- `audit_manifest.csv`: eine Zeile je Messmitteldatensatz, danach eine Zeile je festgeschriebenem Kalibrierereignis. Rund 45 Spalten, darunter Messmittelidentifikation, Standort und Ort, alle Kalibrierfelder, die messtechnischen Felder, die Freigabe- und Prüferfelder, die Auswirkung der Toleranzüberschreitung, die benutzerdefinierten Felder des Arbeitsbereichs als JSON sowie die Werte `record_hash_hex` und `prev_hash_hex`. Die Hash-Spalten sind bewusst vom Schutz gegen Formel-Injektion in CSV ausgenommen, damit sie für den Abgleich der Verkettung bytegenau bleiben.
- `audit_summary.pdf`: ein lesbarer Bericht mit einer Konformitätsübersicht, einem manipulationserkennbaren Abschnitt zur Integritätsprüfung mit dem Urteil über die Kette, der Anzahl der geprüften Einträge, dem Hash-Algorithmus und den Hashes des Genesis- und des neuesten Datensatzes, danach der Audit-Trail der Kalibrierungen, das Messmittelverzeichnis und die Einzelheiten zu Toleranzüberschreitungen. Die Ausnahmetabelle listet die 20 jüngsten zutreffenden Ereignisse auf; die vollständige Menge steht in `audit_manifest.csv`.
- `assets/<tag>/...`: die Nachweisdateien selbst, im Originalformat, gruppiert nach Messmittelkennung.
- Ein README-Prüfleitfaden mit dem Exportumfang, den Abdeckungszahlen, der Erklärung der Hash-Kette und dem Verfahren zur Offline-Prüfung der Verkettung.

Das Archiv soll Ihre Feststellung zu 11.10(b) unterstützen: Es liefert die Aufzeichnungen sowohl in für Menschen lesbarer Form (PDF) als auch in elektronischer Form (CSV). Ob es 11.10(b) für Ihre Aufzeichnungen erfüllt, stellen Sie fest. Es ist auch die praktische Antwort auf Fragen zur Anbieterkontinuität: Das Paket ist in sich geschlossen, im offenen Format, und seine Verkettung ist ohne uns prüfbar.

Umfang und eine wichtige Grenze. Exporte lassen sich nach Standort, Ort, bestimmten Messmitteln, Zeitraum und Status eingrenzen, und der Umfang wird immer mit den Standortberechtigungen der anfragenden Person geschnitten, kann also nur enger werden. **Ein eingegrenzter oder auf einen Zeitraum beschränkter Export prüft den eigenen Hash jedes exportierten Datensatzes erneut, trifft aber keine Aussage über die Kontinuität der Kette zwischen Datensätzen, weil eine gefilterte Menge eine bewusst gewählte Teilmenge der Kette ist.** Nur ein Export ohne Umfang mit der gesamten Historie durchläuft die vollständige Kette. Nutzen Sie einen Export ohne Umfang, wenn Sie den Nachweis der Kontinuität brauchen. Die README sagt das ebenfalls.

Aufbewahrung, solange das Konto aktiv ist: Die Aufzeichnungen werden für die gesamte Lebensdauer des Arbeitsbereichs aufbewahrt. Kein einzelner festgeschriebener Kalibrierdatensatz kann von irgendjemandem bearbeitet oder gelöscht werden, auch nicht von uns.

Aufbewahrung nach der Schließung: Wird ein Konto geschlossen, werden die Daten **730 Tage (etwa 24 Monate)** aufbewahrt, damit Sie sich erneut anmelden und exportieren können. Die Abrechnung wird mit dem Antrag sofort beendet, in dieser Frist wird also nichts berechnet. Nach der Frist löscht eine endgültige Bereinigung die Daten des Arbeitsbereichs in allen Tabellen und entfernt die gespeicherten Nachweisdateien. Diese Bereinigung ist der **einzige** zulässige Weg, auf dem festgeschriebene Journalzeilen je entfernt werden, und sie betrifft immer den ganzen Arbeitsbereich, nie einen einzelnen Datensatz.

Datensicherungen: Die Produktivdatenbank hat automatische tägliche Sicherungen mit einer Aufbewahrungsfrist von 14 Tagen, aktiviertem Löschschutz und einem abschließenden Snapshot beim Abbau jeder Instanz. Was wir über die Wiederherstellung nicht behaupten, steht in Abschnitt 6.

Hosting: Die Produktivumgebung läuft auf Amazon Web Services in us-east-1, USA. Die Datenbank ist im Ruhezustand verschlüsselt und hat keinen Zugang aus dem öffentlichen Internet. Anwendung und API werden ausschließlich über HTTPS mit mindestens TLS 1.2 ausgeliefert. Kontoweites AWS CloudTrail ist mit Integritätsprüfung der Logdateien und einer Aufbewahrungsfrist von 365 Tagen aktiviert. Eine separate Sicherheitsübersicht ist unter axiospec.com/security veröffentlicht.

5. Änderungsmanagement

Wie Änderungen vorgenommen und abgesichert werden.

- Produktiv-Deployments werden **nur manuell ausgelöst**. Es gibt keine automatische Übernahme in die Produktivumgebung.
- Ein Produktiv-Deployment ist gesperrt, solange nicht zuvor drei Jobs bestanden sind: die vollständige Backend-Testsuite, ein Job zur Validierung des OpenAPI-Schemas und eine Schwachstellenprüfung der Abhängigkeiten. Eine fehlgeschlagene Testsuite stoppt das Deployment.
- Die Backend-Testsuite umfasst **2.465 Testfunktionen in 197 Testdateien**. Dazu kommen 233 Testdateien im Web-Frontend. Es sind automatisierte Regressionstests, die bei jeder Änderung laufen.

- Jeder Produktiv-Build wird unter einem unveränderlichen Image-Tag je Commit veröffentlicht, sodass es für jedes Release ein festgelegtes Rollback-Ziel gibt.
- Staging und Produktion sind getrennte Umgebungen mit getrennter Infrastruktur. Änderungen erreichen zuerst Staging.

Klar benannt, was das ist und was nicht. Eine automatisierte Testsuite dieser Größe ist eine echte und zitierbare Kontrolle der Softwareentwicklung und gutes Ausgangsmaterial für eine Argumentation zur Funktionsqualifizierung. Sie ist **kein** Validierungspaket. Sie ist nicht gegen eine formale funktionale Spezifikation geschrieben, es gibt keine Rückverfolgbarkeitsmatrix von Anforderungen zu Tests und keinen unterschriebenen Freigabedatensatz. Ein Prüfer für die Validierung computergestützter Systeme wird sie nicht als solches akzeptieren, und wir werden sie nicht als solches darstellen.

Woran Sie erkennen, dass sich etwas ändert.

Axiospec ist mandantenfähige Software as a Service. Alle Kunden nutzen eine einzige Produktivversion. **Sie können keine Version festschreiben, kein Update aufschieben und kein früheres Release betreiben.** Das ist eine echte Einschränkung für eine validierte Umgebung, und Sie sollten sie in Ihrer Risikobewertung festhalten.

Heute gibt es **kein veröffentlichtes Änderungsprotokoll, keine Seite mit Versionshinweisen und keine schriftliche Zusage zur Benachrichtigung über Änderungen.** Wenn Ihr Verfahren eine Vorankündigung von Änderungen an einem validierten System verlangt, fordern Sie diese Zusage vor dem Kauf schriftlich bei uns an, unter support@axiospec.com. Wir sagen Ihnen lieber, dass es sie nicht gibt, als dass Sie es während eines Audits feststellen.

Was wir Ihnen dazu empfehlen, angesichts des Obigen: Legen Sie in Ihrer Verfahrensanweisung ein regelmäßiges Intervall für die erneute Prüfung fest (zum Beispiel die OQ-Teilmenge vierteljährlich und nach jeder bemerkten Änderung an einer Funktion, auf die Sie sich verlassen, erneut durchführen), und führen Sie im selben Intervall die Kettenprüfung erneut aus und zeichnen Sie das Ergebnis auf. Die Kettenprüfung braucht einen Klick und erzeugt ein datiertes, zuordenbares Ergebnis.

6. Grenzen dessen, was diese Software leistet

Klar benannt, weil sich ein kleiner Anbieter, der seine Grenzen nennt, leichter qualifizieren lässt als einer, der ausweicht.

Zertifizierungen und Bewertungen, die wir nicht besitzen. Kein SOC 2, weder Typ I noch Typ II. Keine ISO/IEC 27001. Kein Penetrationstest durch Dritte. Kein HIPAA Business Associate Agreement, und wir nehmen keine geschützten Gesundheitsinformationen an. Kein FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR oder DFARS 252.204-7012. Wenn Sie mit kontrollierten, nicht als Verschlusssache eingestuften Informationen oder mit exportkontrollierten Daten arbeiten, passt Axiospec derzeit nicht. Kein veröffentlichter Zusatz zur Auftragsverarbeitung, keine Standardvertragsklauseln und keine Datenhaltung in der EU; alle Daten liegen in den USA.

Kein Validierungspaket des Anbieters. Es gibt kein IQ/OQ/PQ-Paket, kein Validierungsprotokoll, keine Rückverfolgbarkeitsmatrix und keinen von uns erstellten zusammenfassenden Validierungsbericht. Abschnitt 3 ist eine Checkliste, die Sie durchführen, kein Nachweis, dass etwas durchgeführt wurde.

Keine Konformitätsaussage. Axiospec zertifiziert, sichert oder garantiert nicht Ihre Konformität mit einer Norm. Es unterstützt und dokumentiert Kalibrieraufzeichnungen und hält sie auditbereit. Die Konformität stellen Ihre Qualitätsstelle, Ihre Zertifizierungsstelle, Ihre Akkreditierungsstelle oder Ihr Inspektor fest.

Wir behaupten keine Konformität mit 21 CFR Part 11. Die Bausteine der Datensatzintegrität sind wirklich stark: von der Datenbank erzwungene Unveränderlichkeit, eine SHA-256-Hash-Kette, zugeordnete Einträge mit Zeitstempel, nur angehängte Korrekturen, die frühere Informationen nicht verdecken, und die Prüfung durch zwei Personen. Die Signaturkontrollen fehlen noch. Siehe Abschnitt 2.4: Die elektronische Signatur ist je Arbeitsbereich optional statt verpflichtend, es gibt keine gespeicherte Signaturbindung am Datensatz, kein Feld für die Bedeutung der Signatur und keine Multi-Faktor-Identifikation. Wir veröffentlichen eine Funktionszuordnung mit markierten Lücken; wir veröffentlichen keine Konformitätsaussage.

Keine Multi-Faktor-Authentifizierung. Es gibt kein eingebautes TOTP, keine Authenticator-App, kein WebAuthn, keine SMS und keine Backup-Codes. Der einzige Weg zu einem zweiten Faktor ist heute die Anmeldung über Google, wo Ihr eigener Identitätsanbieter ihn erzwingt. Enterprise-SSO je Arbeitsbereich über OIDC und SAML ist im Backend gebaut und getestet, aber in der Produktivumgebung nicht aktiviert und sollte als auf Anfrage verfügbar gelten, nicht als ausgelieferte Funktion. Wenn Ihre IT-Richtlinie für alle QM-Systeme erzwungene MFA verlangt, ist das heute ein hartes Ausschlusskriterium. Fragen Sie uns vor dem Kauf nach dem aktuellen Stand.

Änderungen an Stammdatensätzen von Messmitteln werden nicht protokolliert. Abschnitt 2.2 und Test OQ-17. Kalibrierereignisse sind vollständig durch das Journal abgedeckt. Änderungen am beschreibenden Datensatz des Messmittels, einschließlich seines Kalibrierintervalls, werden im Aktivitätsprotokoll nicht zugeordnet.

Gefilterte Exporte belegen keine Kontinuität der Kette. Abschnitt 4. Nutzen Sie dafür einen Export ohne Umfang.

Keine Verfügbarkeitszusage. Es gibt kein Verfügbarkeits-SLA, keine Statusseite und keine veröffentlichte Verfügbarkeitshistorie. Die Produktivdatenbank ist eine einzelne Instanz in einer einzigen Verfügbarkeitszone, sodass ein Ausfall der Verfügbarkeitszone eine Wiederherstellung statt eines Failovers erfordert. Wir veröffentlichen kein Ziel für Wiederherstellungszeit oder Wiederherstellungspunkt, und es wurde keine Wiederherstellungsübung dokumentiert. Sicherungen sind eingerichtet und werden 14 Tage aufbewahrt; das ist eine zutreffende Aussage über Sicherungen, keine belegte Aussage über die Wiederherstellung. Ihre Verfahrensanweisung sollte einen Notfallweg für den Fall enthalten, dass das System nicht verfügbar ist, wonach Begutachter nach ISO/IEC 17025 ohnehin fragen.

Kein dokumentierter Plan zur Reaktion auf Vorfälle und keine vertragliche Frist für Meldungen von Datenschutzverletzungen. Infrastrukturalarme sind in CloudWatch eingerichtet und gehen an eine E-Mail-Adresse für die Rufbereitschaft. Das ist Überwachung, kein Programm zur Reaktion auf Vorfälle.

Keine vom Kunden verwalteten Verschlüsselungsschlüssel. Die Verschlüsselung nutzt von AWS verwaltete Schlüssel.

Datensätze lassen sich nur auf genau einem Weg löschen. Kein einzelner festgeschriebener Datensatz kann von irgendjemandem bearbeitet oder gelöscht werden. Der einzige Löschweg ist eine vom Kunden beantragte Bereinigung des gesamten Arbeitsbereichs nach der Aufbewahrungsfrist von 730 Tagen.

Wir führen keine Kalibrierungen durch. Axiospec ist ein Dokumentationssystem, kein akkreditiertes Kalibrierlaboratorium, und hat keine der Messungen in Ihren Aufzeichnungen durchgeführt.

So nutzen Sie dieses Dokument. Fügen Sie es Ihrer Lieferantenqualifizierung für CaliTech LLC bei (ISO 9001, Abschnitt 8.4; ISO/IEC 17025, Abschnitt 6.6). Verweisen Sie in Ihrem Validierungsplan darauf als die Funktions- und Kontrollbeschreibung des Anbieters. Führen Sie Abschnitt 3 in Ihrem eigenen Arbeitsbereich durch und bewahren Sie das unterschriebene Ergebnis als Ihren Qualifizierungsnachweis auf. Halten Sie die Grenzen aus Abschnitt 6 zusammen mit Ihren ausgleichenden Kontrollen in Ihrer Risikobewertung fest.

Wenn eine Aussage in diesem Dokument nicht zu dem passt, was Sie im Produkt beobachten, teilen Sie es uns unter support@axiospec.com mit, und wir korrigieren das Dokument.
