Sommaire de validation du logiciel

Axiospec, gestion des étalonnages Préparé pour le gestionnaire de la qualité, le responsable de la validation ou l'évaluateur des TI qui évalue Axiospec comme système officiel de dossiers d'étalonnage.

Version du document 1.0. Dernière révision le 2026-08-19. Publié par CaliTech LLC, Knoxville, au Tennessee (États-Unis). Questions : support@axiospec.com, réponse en un jour ouvrable.

À lire d'abord

Ce document est **un intrant de votre dossier de validation. Ce n'est pas un dossier de validation.**

Axiospec ne valide pas votre instance, ne certifie pas votre conformité et n'effectue pas votre qualification. La validation est une détermination que vous faites au sujet de votre propre utilisation prévue, de votre configuration, de vos procédures et de votre personnel. Votre registraire, votre évaluateur ou votre inspecteur décide si vous y avez satisfait.

Ce que ce document vous donne : un énoncé d'utilisation prévue, une description des contrôles d'intégrité des données qui existent dans le produit et de la façon dont ils sont imposés, une liste de vérification que vous pouvez exécuter et signer dans votre propre espace de travail, notre pratique de gestion des changements et une liste claire de ce que le logiciel ne fait pas.

Selon la catégorisation GAMP 5, un registre logiciel-service multilocataire configuré de ce type est normalement traité comme une Catégorie 4 (produit configuré). Cela signifie que votre effort de validation est fondé sur les risques et s'appuie sur la documentation du fournisseur, en plus de vos propres essais de configuration et de processus. Confirmez cette catégorisation selon votre propre procédure.

1. Énoncé d'utilisation prévue

Axiospec est un système de gestion documentaire pour les équipements de mesure et d'essai. Son utilisation prévue consiste à :

- Tenir un registre des instruments, avec leur identification, leur fabricant, leur modèle, leur numéro de série, leur emplacement, leur site et les champs personnalisés définis dans l'espace de travail.
- Enregistrer les événements d'étalonnage et de vérification de ces instruments, y compris les lectures avant ajustage et après ajustage, la valeur nominale, la tolérance, le résultat, les conditions ambiantes, l'étalon de référence utilisé, le numéro de certificat, le fournisseur de services et la référence de traçabilité.
- Enregistrer les champs métrologiques utilisés dans les processus ISO/IEC 17025 : incertitude de mesure, facteur d'élargissement, niveau de confiance, règle de décision, déclaration de conformité et numéro de certificat de l'étalon de référence lui-même.
- Établir le statut d'étalonnage de chaque instrument et sa date de prochaine échéance, et faire ressortir les instruments en retard et ceux qui arrivent bientôt à échéance.

- Conserver ces dossiers en ajout seulement, sous une forme à détection d'altération, avec attribution et horodatage.
- Faire passer les dossiers d'étalonnage par une approbation facultative à deux personnes avant qu'ils prennent effet.
- Produire une exportation complète, lisible par l'humain et par la machine, du registre et de son historique pour l'audit.

Axiospec **n'est pas** un laboratoire d'étalonnage accrédité et n'effectue aucune mesure. Chaque document produit par le système porte textuellement cette mention :

> « Données d'étalonnage saisies par le personnel de l'espace de travail. Axiospec est un système de gestion documentaire, non un laboratoire d'étalonnage accrédité, et n'a pas réalisé cette mesure. »

Axiospec n'est pas un logiciel de dispositif médical, et aucune pertinence au regard de l'IEC 62304 n'est revendiquée ni sous-entendue. L'IEC 62304 régit les logiciels qui sont un dispositif médical ou qui en font partie. Un registre d'étalonnages est un outil du système qualité.

Quels articles déterminent les attentes envers un tel système

Le texte des articles des normes ISO est protégé par le droit d'auteur; ce qui suit est donc une série de références d'articles accompagnées d'une paraphrase, et non des citations. Vérifiez-les dans votre propre exemplaire sous licence.

- **ISO 9001:2015, article 7.1.5.2** (traçabilité de la mesure) : équipements étalonnés ou vérifiés à des intervalles spécifiés par rapport à des étalons traçables, identifiables quant à leur statut d'étalonnage, protégés contre les réglages qui invalideraient le résultat, et évaluation des résultats antérieurs lorsqu'un équipement est jugé inapte.
- **ISO 9001:2015, article 7.5.3** (maîtrise de l'information documentée) : disponibilité, protection contre la perte d'intégrité, contrôle de l'accès, stockage et préservation, maîtrise des modifications et des versions, conservation et élimination.
- **ISO 9001:2015, article 8.4** et **ISO/IEC 17025:2017, article 6.6** (produits et services fournis par des prestataires externes) : vous devez évaluer et consigner votre qualification d'Axiospec comme fournisseur. Ce document est conçu pour servir de preuve dans ce dossier.
- **ISO/IEC 17025:2017, article 6.4** (équipements), en particulier 6.4.6 (étalonnage lorsque l'exactitude ou l'incertitude influe sur la validité), 6.4.8 (étiquetage ou codage du statut pour que l'utilisateur reconnaisse facilement le statut d'étalonnage ou la période de validité) et 6.4.13 (le contenu exigé des enregistrements relatifs aux équipements).
- **ISO/IEC 17025:2017, article 7.11** (maîtrise des données et gestion de l'information), en particulier 7.11.2 (le système de gestion de l'information est validé quant à sa fonctionnalité, y compris les interfaces) et 7.11.3 (protégé contre l'accès non autorisé, protégé contre l'altération et la perte, exploité selon sa spécification, entretenu de façon à garantir l'intégrité des données, avec consignation des défaillances et des mesures correctives).
- **ISO 13485:2016, article 4.1.6** : procédures de validation des logiciels utilisés dans le SMQ, avant la première utilisation et après les changements, selon une approche proportionnée au risque, avec

conservation des enregistrements.

- **21 CFR Part 11**, lorsque les dossiers d'étalonnage sont vos dossiers réglementés officiels : 11.10(a) validation, 11.10(b) copies exactes et complètes sous forme lisible par l'humain et sous forme électronique, 11.10(c) protection et récupération rapide, 11.10(d) accès limité aux personnes autorisées, 11.10(e) pistes d'audit sécurisées, générées par ordinateur et horodatées, où « les modifications des dossiers ne doivent pas masquer l'information enregistrée précédemment », 11.10(g) vérifications d'autorité, 11.50 manifestations de la signature, 11.70 lien entre la signature et le dossier.

Notez que l'ISO 9001 ne contient aucun article explicite sur la validation des logiciels. Pour une entreprise qui applique seulement la 9001, l'obligation porte sur la maîtrise de l'information documentée, et non sur un protocole de validation. Dimensionnez votre effort en conséquence.

2. Contrôles d'intégrité des données qui existent

2.1 Registre d'étalonnage en ajout seulement, à détection d'altération

Chaque événement d'étalonnage est écrit dans un registre. Dès qu'une entrée est confirmée (c'est-à-dire dès qu'elle quitte l'état de brouillon, DRAFT), elle ne peut plus être ni modifiée ni supprimée.

Comment fonctionne la détection d'altération. Chaque entrée confirmée stocke un `record_hash` : une empreinte SHA-256 calculée sur une sérialisation JSON canonique, à clés triées, des champs de cette entrée, qui inclut le `record_hash` de l'entrée précédente sous le nom `prev_hash`. Les entrées sont enchaînées par espace de travail dans l'ordre d'insertion, avec `created_at` forcé à être strictement croissant, de sorte que l'ordre est une relecture déterministe. Toute modification, insertion ou suppression d'un enregistrement change son empreinte et brise la chaîne à partir de ce point, et la rupture est détectable.

Les champs intégrés à l'empreinte sont : l'actif, le type d'événement, l'horodatage de réalisation, l'utilisateur qui l'a effectué, le résultat de l'étalonnage, la valeur nominale, la tolérance, les lectures avant ajustage et après ajustage, la température, l'humidité, l'étalon de référence, les mesures, les notes, la référence de la pièce jointe, le numéro de certificat, le fournisseur de services, la référence de traçabilité, le motif de correction et les champs métrologiques énumérés à la section 1.

Les fichiers de preuve sont intégrés à l'empreinte par leur contenu, pas seulement par leur référence. L'empreinte SHA-256 du certificat ou de la photo téléversés est calculée côté serveur et intégrée à l'empreinte de l'enregistrement. Remplacer le fichier derrière un lien inchangé brise la chaîne.

L'immuabilité est imposée par la base de données, pas par le code de l'application. Un déclencheur PostgreSQL sur la table du registre bloque, au niveau de la base de données : la suppression d'une entrée confirmée, le retour d'une entrée confirmée à l'état de brouillon et la modification de toute colonne d'identité ou intégrée à l'empreinte d'une entrée confirmée. Cela signifie qu'une session SQL directe sur la base de données de production ne peut pas réécrire en silence un dossier d'étalonnage. C'est un contrôle plus fort qu'une vérification dans la couche applicative, et c'est précisément le point qui vaut la peine d'être démontré à un évaluateur.

Les changements sont représentés par ajout, jamais par écrasement. C'est la réponse directe à l'exigence de la Part 11 voulant que les modifications des dossiers ne masquent pas l'information

enregistrée précédemment.

- Une **correction** est une nouvelle entrée ajoutée qui renvoie à l'entrée qu'elle remplace et porte un motif de correction en texte libre. Le motif est obligatoire (l'API rejette une correction sans motif) et fait lui-même partie de l'empreinte. L'entrée remplacée reste dans l'historique, entièrement lisible.
- Une **annulation** est un événement marqueur ajouté au registre. L'original annulé reste dans l'historique avec la pastille annulé, et l'instrument revient à son étalonnage précédent ou à non étalonné. Une annulation ne peut jamais compter comme un étalonnage.

Vérification en un clic. Tout utilisateur authentifié de l'espace de travail peut lancer une vérification complète de la chaîne, qui parcourt chaque entrée confirmée, recalcule chaque empreinte, vérifie la continuité et indique soit un résultat sans anomalie avec le nombre d'entrées vérifiées, soit la première entrée non concordante avec l'étiquette de son instrument. Le résultat et l'utilisateur qui a vérifié sont enregistrés.

Vérification indépendante hors de la plateforme. L'exportation d'audit contient les valeurs `record_hash` et `prev_hash` dans le CSV du manifeste, ainsi qu'un README qui décrit étape par étape comment vérifier hors ligne l'**enchaînement** de la chaîne sans Axiospec : le `prev_hash_hex` de chaque ligne doit être égal au `record_hash_hex` de la ligne précédente, de sorte que tout enregistrement supprimé, inséré ou réordonné apparaît comme un lien brisé. Il faut être précis sur la limite. Le manifeste ne contient pas tous les champs qui alimentent la fonction de hachage, donc il est impossible de recalculer l'empreinte d'un enregistrement à partir du seul CSV. Le recalcul de l'empreinte d'un enregistrement individuel se fait côté serveur, dans l'application et au moment de l'exportation. L'enchaînement est ce que vous pouvez prouver vous-même, sans nous, pour toujours.

2.2 Piste d'audit

Dossiers d'étalonnage. Chaque entrée stocke l'identifiant de l'utilisateur qui l'a effectuée ainsi qu'un instantané figé de son nom, l'horodatage de réalisation et l'horodatage de création côté serveur. Quand l'entrée passe en révision, elle stocke aussi l'identifiant et l'instantané du nom du réviseur, l'horodatage de la révision, les notes de révision et, le cas échéant, le motif de rejet. Les valeurs antérieures sont préservées par construction : rien n'est écrasé, donc la « valeur précédente » est l'entrée remplacée, toujours lisible.

Administration de l'espace de travail. Un journal d'activité distinct enregistre les actions liées à l'équipe et à la configuration avec l'utilisateur qui agit, la cible, un enregistrement JSON de ce qui a changé, l'adresse IP source et un horodatage. Les actions couvertes comprennent les invitations et révocations d'utilisateurs, les changements de rôle, l'archivage d'utilisateurs, les changements d'adresse courriel, l'émission et la révocation de clés d'API, les modifications de la configuration SSO et les connexions SSO, les modifications d'abonnements aux webhooks et le début d'une période d'essai de la facturation. Les administrateurs de l'espace de travail peuvent le consulter dans l'application, strictement limité à l'espace de travail de la session authentifiée et non à un paramètre de requête.

Lacune connue, déclarée. Les modifications de la fiche maître d'un instrument (par exemple son intervalle d'étalonnage) ne sont pas encore consignées dans le journal d'audit du système. Les événements d'étalonnage eux-mêmes sont immuables et entièrement attribués. Il en va de même pour l'étiquette, le numéro de série et l'emplacement d'un instrument. Si votre procédure doit savoir « qui a modifié l'intervalle

de cet instrument et quand », vous devez le couvrir au moyen de votre propre contrôle jusqu'à ce que cette lacune soit comblée. Voir la section 6.

2.3 Approbations (rédacteur et réviseur)

La révision à deux personnes est offerte par instrument ou pour tout l'espace de travail. Elle est **facultative et désactivée par défaut.**

Quand la révision est exigée, le système refuse que la personne qui soumet approuve son propre dossier. La vérification est inconditionnelle au début des deux voies, approbation et rejet, et elle échoue aussi en position fermée si l'identité de l'approbateur ne peut pas être établie. L'approbation exige le rôle de gestionnaire ou d'administrateur, vérifié à la fois pour toute l'organisation et au site précis auquel appartient l'instrument, de sorte qu'un gestionnaire de toute l'organisation rétrogradé à ce site y est refusé. La route générique de mise à jour des dossiers refuse de fixer un statut approuvé ou rejeté, donc le flux de travail ne peut pas être contourné. Les annulations suivent le même flux de travail, et une annulation en attente ou rejetée ne masque pas l'original.

Quand la révision **n'est pas** exigée, la soumission est approuvée automatiquement et la personne qui soumet est enregistrée comme approbateur. Une seule personne enregistre et le dossier prend effet immédiatement. Indiquez-le clairement dans votre propre évaluation des risques, et activez la révision pour les instruments où votre évaluation des risques l'exige.

2.4 Signatures électroniques

Ce qui est réel et offert. La signature électronique est un paramètre par espace de travail. Elle est facultative, pas obligatoire. Quand un espace de travail l'active, l'approbation exige que le mot de passe du propre compte de l'approbateur soit vérifié de nouveau au moment de la signature, côté serveur, par rapport à l'empreinte du mot de passe stockée, avant que l'approbation se poursuive. Un mauvais mot de passe est toujours refusé avec une erreur 403, peu importe le réglage de configuration. L'application mobile demande le mot de passe quand un étalonnage est enregistré. Les mots de passe sont stockés en PBKDF2-HMAC-SHA256 avec 260 000 itérations et un sel aléatoire de 16 octets par mot de passe, et la vérification se fait en temps constant. Un point de terminaison de réauthentification distinct existe dans le même but. L'utilisateur qui approuve et l'horodatage de l'approbation sont consignés dans l'enregistrement immuable du registre, figés par le déclencheur de la base de données décrit à la section 2.1.

Deux limites à connaître avant de vous y fier.

1. **Elle est facultative par espace de travail et n'est pas imposée de façon stricte pour l'instant.** Si le client n'envoie aucun mot de passe de signature, l'approbation réussit actuellement et consigne un avertissement, au lieu d'être refusée. Seul un mauvais mot de passe est refusé. L'interrupteur d'application stricte existe dans le code, mais il n'est pas activé dans l'environnement de production.
2. **Il n'existe aucun lien cryptographique de signature stocké.** Ne vous attendez pas à un artefact de signature distinct et récupérable dans le dossier d'étalonnage, ni à un indicateur « signé » dans l'API. La preuve durable est le dossier d'approbation lui-même : l'identité de l'approbateur, l'instantané de son nom, l'horodatage de l'approbation et les notes de révision, tous figés par le déclencheur d'immuabilité.

Par conséquent, Axiospec **ne satisfait pas** actuellement aux articles 11.50 et 11.70 du 21 CFR, et l'attente de deux composants d'identification distincts pour les sessions non continues ne peut pas être satisfaite,

puisque le produit n'offre pas d'authentification multifacteur. Si les signatures électroniques au sens de la Part 11 sont une exigence ferme pour vous, traitez ce point comme une lacune et soulevez-le avec nous avant d'acheter.

2.5 Contrôle d'accès fondé sur les rôles

Cinq rôles : super-administrateur, administrateur, gestionnaire, technicien, auditeur. L'application des droits se fait **côté serveur**, sur chaque route, au moyen des dépendances FastAPI. Le rôle de l'utilisateur est déterminé de nouveau à partir de la base de données au moment de la requête plutôt que d'être tiré du jeton de session, de sorte qu'un jeton périmé ne peut pas conserver des privilèges élevés. Il existe aussi des restrictions côté client, mais elles sont cosmétiques; le serveur est le point d'application.

Comportements pertinents pour 11.10(d) et (g) et pour l'ISO/IEC 17025 7.11.3 :

- Le pouvoir de modifier les rôles est encadré. Un gestionnaire ne peut gérer que des techniciens. Les droits d'invitation sont limités selon le rôle.
- **Le rôle d'auditeur est imposé en lecture seule dans tout le système.** Toutes les méthodes HTTP d'écriture sont bloquées pour les auditeurs, avec exactement deux exceptions permises : demander une exportation de la piste d'audit et révoquer son propre jeton de flux de calendrier (ce qui retire un accès et n'en accorde jamais). C'est le rôle à attribuer à votre registraire ou à un évaluateur externe.
- Une **frontière d'accès par site** s'ajoute au rôle. Un utilisateur peut détenir un rôle à l'échelle de l'organisation et quand même se voir refuser l'accès à un site précis, et cela est vérifié lors de la soumission, de l'annulation et de l'approbation d'étalonnages.
- Seuls les gestionnaires et les administrateurs peuvent annuler un étalonnage. Les techniciens ne peuvent corriger que leurs propres dossiers; les gestionnaires et les administrateurs peuvent corriger n'importe lequel.

Les dossiers sont stockés avec un cloisonnement par espace de travail au niveau des lignes, imposé dans la couche d'accès aux données, l'espace de travail étant tiré d'une revendication de session dont la signature est vérifiée, jamais d'un en-tête fourni par le client. Notez la description honnête : il s'agit d'un cloisonnement par espace de travail **imposé par l'application**, pas de la sécurité au niveau des lignes de PostgreSQL, ni d'une base de données distincte par client. L'immuabilité du registre, en revanche, est imposée par la base de données.

3. Ce que vous devriez vérifier dans votre propre environnement

Ce qui suit est un protocole suggéré que vous exécutez et consignez. Rien ici n'a été exécuté pour vous. Pour chaque étape, consignez la date, la personne qui l'a exécutée, le résultat attendu, le résultat obtenu, la conformité ou non, et joignez une capture d'écran. Au sens de l'ISO/IEC 17025 7.11.2, c'est la vérification fonctionnelle qui vous revient.

Qualification d'installation (IQ), configuration consignée

No	Vérification	Consignation
IQ-1	Nom de l'espace de travail, URL de l'application et date de la première utilisation en production	

No	Vérification	Consignation
IQ-2	Utilisateurs nommés, leurs rôles et leurs droits par site	
IQ-3	Paramètres de l'espace de travail consignés : approbations exigées oui/non, signature électronique activée/désactivée, modules activés, champs personnalisés définis	
IQ-4	Sites et emplacements configurés, conformes à votre liste d'installations	
IQ-5	Registre des instruments chargé, nombre rapproché de votre registre source	
IQ-6	Dossier de qualification de fournisseur ouvert pour CaliTech LLC, avec ce document en pièce jointe	
IQ-7	Votre procédure contrôlée qui désigne Axiospec comme système de dossiers d'étalonnage, émise et approuvée dans le cadre de votre contrôle documentaire	

Qualification opérationnelle (OQ), essais fonctionnels

No	Essai	Résultat attendu
OQ-1	Enregistrer un étalonnage sur un instrument d'essai	L'entrée apparaît dans l'historique de cet instrument avec votre nom, la date de réalisation et les lectures saisies
OQ-2	Tenter de modifier ce dossier confirmé	Le système refuse et vous invite à émettre une correction
OQ-3	Tenter de supprimer ce dossier confirmé	Le système refuse en indiquant que le registre est en ajout seulement
OQ-4	Émettre une correction sans motif, puis avec un motif	Refusée sans motif; acceptée avec un motif; l'entrée d'origine reste visible dans l'historique
OQ-5	En tant que gestionnaire, annuler un étalonnage	L'original reste dans l'historique avec la pastille annulé; le statut de l'instrument revient à l'étalonnage précédent ou à non étalonné
OQ-6	En tant que technicien, tenter d'annuler un étalonnage	Refusé
OQ-7	Activer l'approbation pour un instrument. Soumettre un étalonnage en tant qu'utilisateur A, puis tenter de l'approuver en tant qu'utilisateur A	Refusé, en invoquant la séparation entre rédacteur et réviseur
OQ-8	L'approuver en tant qu'utilisateur B	Le nom de l'approbateur et l'horodatage de l'approbation sont consignés dans l'entrée et visibles dans l'historique

No	Essai	Résultat attendu
OQ-9	Se connecter avec un utilisateur qui a le rôle d'auditeur et tenter une modification quelconque	Toutes les écritures sont refusées
OQ-10	Affecter un utilisateur au Site 1 seulement, puis tenter d'agir sur un instrument du Site 2	Refusé
OQ-11	Lancer la vérification de la chaîne à partir de la section d'audit	Indique « vérifiée », avec le nombre d'entrées vérifiées. Consignez la date, le nombre et l'utilisateur qui a vérifié
OQ-12	Générer une exportation d'audit sans portée	Un fichier ZIP est téléchargé, qui contient audit_manifest.csv, audit_summary.pdf, le guide de vérification README et les fichiers joints
OQ-13	Suivre la procédure du README pour vérifier l'enchaînement hors ligne	Le `prev_hash_hex` de chaque ligne est égal au `record_hash_hex` de la ligne précédente
OQ-14	Enregistrer un résultat hors tolérance	L'instrument est signalé; l'évaluation de l'impact du hors tolérance peut être saisie une fois, puis elle est verrouillée
OQ-15	Confirmer que le statut d'étalonnage et la date de prochaine échéance s'affichent correctement pour un instrument connu (ISO/IEC 17025 6.4.8)	Le statut et l'échéance correspondent à ce que vous attendez
OQ-16	Changer le rôle d'un utilisateur, puis ouvrir le journal d'activité de l'espace de travail	Le changement apparaît avec l'utilisateur qui a agi, la cible et l'horodatage
OQ-17	Modifier l'intervalle d'étalonnage d'un instrument, puis consulter le journal d'activité	**Aucune entrée n'apparaît. C'est la lacune connue de la section 2.2.** Consignez-la comme lacune de contrôle et documentez votre contrôle compensatoire
OQ-18	Imprimer ou exporter un certificat d'étalonnage pour un dossier approuvé, puis tenter la même chose pour un dossier annulé	Le certificat est produit pour le dossier approuvé; il est refusé pour le dossier annulé

Qualification de performance (PQ), votre processus avec votre personnel

No	Activité
PQ-1	Définir la période (un cycle d'étalonnage complet est préférable; un mois est un minimum courant)
PQ-2	Fonctionner en parallèle avec votre registre actuel pendant cette période. Rapprocher à la fin le nombre d'instruments et les échéances
PQ-3	Confirmer que les avis d'échéance et de retard parviennent aux bonnes personnes selon le calendrier prévu
PQ-4	Confirmer que vos techniciens peuvent remplir un dossier d'étalonnage selon votre procédure, sans solution de contournement

No	Activité
PQ-5	Faire un audit simulé. Choisir un instrument au hasard et produire : l'historique complet, la référence de traçabilité, l'étalon de référence utilisé, les pièces jointes de preuve et la preuve que le dossier n'a pas été modifié
PQ-6	Traiter de bout en bout un véritable événement hors tolérance, y compris l'évaluation de l'impact sur les mesures antérieures (ISO 9001 7.1.5.2)
PQ-7	Vérifier la voie de secours prévue dans votre procédure pour les périodes où le système n'est pas disponible
PQ-8	Rédiger et approuver le rapport sommaire de validation. Le signer

Requalification. Définissez ce qui déclenche un nouvel essai. Une règle pratique pour un logiciel-service de Catégorie 4 : exécuter de nouveau le sous-ensemble de l'OQ qui touche toute fonction sur laquelle vous vous appuyez chaque fois que vous modifiez de façon importante votre configuration (paramètres d'approbation, rôles, sites, champs personnalisés, adaptation aux normes), ainsi qu'à un intervalle de révision périodique que vous fixez. Voir la section 5 pour le fonctionnement des changements du côté du fournisseur.

4. Conservation et exportation des dossiers

L'exportation est en libre-service, complète, et n'est liée ni à un forfait payant ni à une demande de soutien. Les gestionnaires, administrateurs et auditeurs peuvent la générer. Les techniciens conservent l'historique par instrument dans l'application, mais pas l'exportation de tout l'espace de travail.

L'exportation est un seul fichier ZIP qui contient :

- `audit_manifest.csv` : une ligne par fiche d'instrument, puis une ligne par événement d'étalonnage confirmé. Environ 45 colonnes, notamment l'identification de l'instrument, le site et l'emplacement, tous les champs d'étalonnage, les champs métrologiques, les champs d'approbation et de réviseur, l'impact du hors tolérance, les champs personnalisés de l'espace de travail en JSON, ainsi que les valeurs `record_hash_hex` et `prev_hash_hex`. Les colonnes d'empreinte sont exclues à dessein de la protection contre l'injection de formules CSV, pour qu'elles soient exactes à l'octet près lors de la comparaison de l'enchaînement.
- `audit_summary.pdf` : un rapport lisible avec un tableau de bord de conformité, une section de vérification d'intégrité à détection d'altération qui indique le verdict sur la chaîne, le nombre d'entrées vérifiées, l'algorithme de hachage et les empreintes de l'enregistrement initial et du plus récent, puis la piste d'audit des étalonnages, le registre des instruments et le détail des cas hors tolérance. Le tableau des exceptions présente les 20 événements visés les plus récents; l'ensemble complet se trouve dans `audit_manifest.csv`.
- `assets/<tag>/...` : les fichiers de preuve eux-mêmes, dans leur format d'origine, regroupés par étiquette d'instrument.
- Un guide de vérification README avec la portée de l'exportation, les nombres couverts, l'explication de la chaîne d'empreintes et la procédure de vérification hors ligne de l'enchaînement.

L'archive est conçue pour appuyer votre détermination au titre de 11.10(b) : elle fournit les dossiers à la fois sous forme lisible par l'humain (PDF) et sous forme électronique (CSV). La question de savoir si elle satisfait à 11.10(b) pour vos dossiers relève de votre détermination. C'est aussi la réponse pratique aux questions sur la continuité du fournisseur : le dossier est autonome, en format ouvert, et son enchaînement se vérifie sans nous.

Portée et une limite importante. Les exportations peuvent être limitées par site, emplacement, instruments précis, période et statut, et la portée est toujours croisée avec les droits par site de la personne qui fait la demande, donc elle ne peut que se resserrer. **Une exportation limitée ou restreinte à une période revérifie l'empreinte propre à chaque enregistrement exporté, mais n'affirme pas la continuité de la chaîne entre les enregistrements, parce qu'un ensemble filtré est un sous-ensemble délibéré de la chaîne.** Seule une exportation sans portée, qui couvre tout l'historique, parcourt la chaîne complète. Utilisez une exportation sans portée quand vous avez besoin de la preuve de continuité. Le README l'indique aussi.

Conservation tant que le compte est actif : les dossiers sont conservés pendant toute la durée de vie de l'espace de travail. Aucun dossier d'étalonnage confirmé ne peut être modifié ou supprimé individuellement par qui que ce soit, nous compris.

Conservation après la fermeture : quand un compte est fermé, les données sont conservées **730 jours (environ 24 mois)** pour que vous puissiez vous reconnecter et exporter. La facturation est annulée dès la demande, donc rien n'est facturé pendant cette période. À la fin de celle-ci, une purge définitive supprime les données de l'espace de travail dans toutes les tables et efface les fichiers de preuve stockés. Cette purge est la **seule** voie autorisée par laquelle des lignes confirmées du registre sont supprimées, et c'est une opération qui porte sur tout l'espace de travail, jamais une suppression dossier par dossier.

Sauvegardes : la base de données de production dispose de sauvegardes quotidiennes automatiques avec une période de conservation de 14 jours, d'une protection contre la suppression activée et d'un instantané final lors de tout démantèlement d'instance. Voir la section 6 pour ce que nous n'affirmons pas au sujet de la reprise.

Hébergement : la production fonctionne sur Amazon Web Services, dans us-east-1, aux États-Unis. La base de données est chiffrée au repos et n'a aucun accès à partir d'Internet. L'application et l'API sont servies uniquement en HTTPS, avec TLS 1.2 au minimum. AWS CloudTrail est activé sur tout le compte avec validation de l'intégrité des fichiers journaux et une période de conservation de 365 jours. Une présentation distincte de la sécurité est publiée à axiospec.com/security.

5. Gestion des changements

Comment les changements sont faits et encadrés.

- Les déploiements en production sont **déclenchés uniquement à la main**. Il n'y a aucune mise en production automatique.
- Un déploiement en production est bloqué tant que trois tâches n'ont pas réussi : la suite complète d'essais du serveur, une tâche de validation du schéma OpenAPI et un audit des vulnérabilités des dépendances. Une suite d'essais en échec arrête le déploiement.

- La suite d'essais du serveur compte **2 465 fonctions d'essai réparties dans 197 fichiers d'essai**. Il existe aussi 233 fichiers d'essai pour l'interface Web. Ce sont des essais de régression automatisés qui s'exécutent à chaque changement.
- Chaque version de production est publiée sous une étiquette d'image immuable par commit, ce qui donne une cible de retour en arrière définie pour chaque version.
- La préproduction et la production sont des environnements distincts, avec une infrastructure distincte. Les changements arrivent d'abord en préproduction.

Soyons clairs sur ce que c'est et ce que ce n'est pas. Une suite d'essais automatisés de cette taille est une mesure réelle et citable de contrôle du développement logiciel, et une bonne matière première pour un argumentaire de qualification opérationnelle. Ce **n'est pas** un dossier de validation. Elle n'est pas écrite à partir d'une spécification fonctionnelle formelle, il n'existe aucune matrice de traçabilité des exigences vers les essais et il n'existe aucun dossier de mise en production signé. Un évaluateur en validation de systèmes informatisés ne l'acceptera pas comme tel, et nous ne la présenterons pas comme telle.

Comment vous savez que quelque chose change.

Axiospec est un logiciel-service multilocataire. Tous les clients utilisent une seule version de production. **Vous ne pouvez pas figer une version, reporter une mise à jour ni exploiter une version antérieure.** C'est une contrainte réelle pour un environnement validé, que vous devriez consigner dans votre évaluation des risques.

Il n'existe actuellement **aucun journal des modifications publié, aucune page de notes de version et aucun engagement écrit de notification des changements.** Si votre procédure exige un préavis pour les changements apportés à un système validé, demandez-nous cet engagement par écrit avant d'acheter, à support@axiospec.com. Nous préférons vous dire qu'il n'existe pas plutôt que de vous le laisser découvrir pendant un audit.

Ce que nous vous suggérons de faire, compte tenu de ce qui précède : définissez dans votre procédure un intervalle de revérification périodique (par exemple, exécuter de nouveau le sous-ensemble de l'OQ chaque trimestre et après tout changement que vous remarquez dans une fonction dont vous dépendez), et relancez la vérification de la chaîne en consignant le résultat au même intervalle. La vérification de la chaîne se fait en un clic et produit un résultat daté et attribuable.

6. Limites de ce que fait ce logiciel

Dites clairement, parce qu'un petit fournisseur qui nomme ses limites est plus facile à qualifier qu'un fournisseur qui les esquive.

Certifications et évaluations que nous ne détenons pas. Aucun SOC 2, ni Type I ni Type II. Aucune ISO/IEC 27001. Aucun test d'intrusion réalisé par un tiers. Aucune entente d'associé d'affaires au sens de la HIPAA, et nous n'acceptons pas de renseignements de santé protégés. Aucun FedRAMP, StateRAMP, CMMC, NIST 800-171, ITAR, EAR ou DFARS 252.204-7012. Si vous traitez des renseignements non classifiés contrôlés ou des données soumises au contrôle des exportations, Axiospec ne vous convient pas pour l'instant. Aucun addenda sur le traitement des données publié, aucune clause contractuelle type et aucune résidence des données dans l'UE; toutes les données se trouvent aux États-Unis.

Aucun dossier de validation du fournisseur. Il n'existe aucun dossier IQ/OQ/PQ, aucun protocole de validation, aucune matrice de traçabilité et aucun rapport sommaire de validation produits par nous. La section 3 est une liste de vérification que vous exécutez, pas la preuve que quoi que ce soit a été exécuté.

Aucune déclaration de conformité. Axiospec ne certifie, n'assure ni ne garantit votre conformité à aucune norme. Il soutient et documente les dossiers d'étalonnage et les garde prêts pour l'audit. La conformité est déterminée par votre service de la qualité, votre registraire, votre organisme d'accréditation ou votre inspecteur.

Nous ne revendiquons pas la conformité au 21 CFR Part 11. Les éléments qui fondent l'intégrité des dossiers sont vraiment solides : immuabilité imposée par la base de données, chaîne d'empreintes SHA-256, entrées attribuées et horodatées, corrections en ajout seulement qui ne masquent pas l'information antérieure, et révision à deux personnes. Les contrôles de signature ne sont pas encore là. Voir la section 2.4 : la signature électronique est facultative par espace de travail plutôt qu'obligatoire, il n'y a aucun lien de signature stocké dans le dossier, aucun champ qui indique la signification de la signature et aucune identification multifacteur. Nous publions une correspondance des fonctionnalités où les lacunes sont indiquées; nous ne publions pas de déclaration de conformité.

Aucune authentification multifacteur. Il n'y a ni TOTP intégré, ni application d'authentification, ni WebAuthn, ni texto, ni codes de secours. Pour l'instant, la seule voie vers un deuxième facteur est la connexion par Google, où votre propre fournisseur d'identité l'impose. L'authentification unique (SSO) d'entreprise par espace de travail au moyen d'OIDC et de SAML est développée et mise à l'essai sur le serveur, mais elle n'est pas activée en production et doit être considérée comme offerte sur demande, et non comme une fonctionnalité livrée. Si votre politique des TI exige une MFA imposée pour tous les systèmes du SMQ, c'est pour l'instant un obstacle absolu. Demandez-nous où en sont les choses avant d'acheter.

Les modifications de la fiche maître des actifs ne sont pas journalisées. Section 2.2 et essai OQ-17. Les événements d'étalonnage sont entièrement couverts par le registre. Les modifications de la fiche descriptive de l'instrument, y compris son intervalle d'étalonnage, ne sont pas attribuées dans le journal d'activité.

Les exportations filtrées ne prouvent pas la continuité de la chaîne. Section 4. Utilisez une exportation sans portée à cette fin.

Aucun engagement de disponibilité. Il n'y a aucune entente de niveau de service (SLA) sur la disponibilité, aucune page d'état et aucun historique de disponibilité publié. La base de données de production est une instance unique dans une seule zone de disponibilité, donc une panne de zone de disponibilité exige une restauration plutôt qu'un basculement. Nous ne publions aucun objectif de délai de reprise ni de point de reprise, et aucun exercice de restauration n'a été documenté. Les sauvegardes sont configurées et conservées 14 jours; c'est un énoncé vrai au sujet des sauvegardes, pas un énoncé démontré au sujet de la reprise. Votre procédure devrait prévoir une solution de secours pour les périodes où le système n'est pas disponible, ce que les évaluateurs ISO/IEC 17025 demandent de toute façon.

Aucun plan documenté d'intervention en cas d'incident ni délai contractuel de notification des atteintes. Des alarmes d'infrastructure sont configurées dans CloudWatch et envoyées à une adresse courriel de garde. C'est de la surveillance, pas un programme d'intervention en cas d'incident.

Aucune clé de chiffrement gérée par le client. Le chiffrement utilise des clés gérées par AWS.

Les dossiers ne peuvent être supprimés que d'une seule façon. Aucun dossier confirmé ne peut être modifié ou supprimé individuellement par qui que ce soit. La seule voie de suppression est une purge de tout l'espace de travail demandée par le client, après la période de conservation de 730 jours.

Nous n'effectuons pas d'étalonnage. Axiospec est un système de gestion documentaire, pas un laboratoire d'étalonnage accrédité, et n'a effectué aucune des mesures de vos dossiers.

Comment utiliser ce document. Joignez-le à votre dossier de qualification de fournisseur pour CaliTech LLC (ISO 9001, article 8.4; ISO/IEC 17025, article 6.6). Citez-le dans votre plan de validation comme la description fonctionnelle et des contrôles fournie par le fournisseur. Exécutez la section 3 dans votre propre espace de travail et conservez le résultat signé comme preuve de qualification. Consignez les limites de la section 6 dans votre évaluation des risques, avec vos contrôles compensatoires.

Si un énoncé de ce document ne correspond pas à ce que vous observez dans le produit, dites-le-nous à support@axiospec.com et nous corrigerons le document.
