TC-04

CONFORMITÉ

Feuille de route de conformité

État d'avancement des démarches de certification et d'alignement réglementaire de CaliaLabs et de l'infrastructure CEREBRO.

Résumé exécutif

> /// EXECUTIVE SUMMARY
>
> CaliaLabs conçoit ses architectures pour répondre nativement aux exigences des environnements financiers et institutionnels. Les démarches de certification présentées dans ce document traduisent cet engagement en jalons opérationnels vérifiables.
>
> Ce document détaille l'état d'avancement de chaque démarche, les partenaires impliqués, les dates cibles, et les prérequis techniques déjà en place. Il est mis à jour à chaque jalon significatif.
>
> Les certifications ne sont pas des objectifs en elles-mêmes. Elles sont la traduction formalisée de propriétés que les architectures CEREBRO doivent démontrer pour pouvoir servir des clients régulés : intégrité des contrôles, traçabilité des décisions, résilience opérationnelle, gouvernance des données.

Points clés

SOC 2 TYPE I

Prévu au troisième trimestre 2026 — revue initiale des contrôles

SOC 2 TYPE II

Prévu au quatrième trimestre 2026 — évaluation opérationnelle sur 6 mois

ISO/IEC 27001

Prévu au quatrième trimestre 2026 — certification SMSI

DORA

Aligné — architecture conforme aux exigences de l'Article 30

RGPD

Natif — privacy by design intégré dès la conception

SÉCURITÉ TRANSPORT

HSTS Preload actif — TLS 1.3 exclusivement

1. Principe de conformité par conception

Les certifications de sécurité et de conformité ne sont pas traitées comme une couche externe ajoutée au produit. Elles sont considérées comme des propriétés qui doivent émerger de l'architecture elle-même.

Cette approche repose sur trois principes : les contrôles réglementaires sont traduits en exigences techniques vérifiables dès la conception, la traçabilité et l'auditabilité sont natives — les journaux ne sont pas reconstruits a posteriori, les tests automatisés vérifient en continu que les propriétés attendues sont préservées à chaque évolution.

Cette discipline évite les situations classiques où la conformité est obtenue au prix d'un empilement de contrôles manuels, fragiles, et coûteux à maintenir.

2. SOC 2 Type I — Troisième trimestre 2026

SOC 2 Type I est une évaluation indépendante des contrôles de sécurité et de disponibilité à un instant donné. Elle atteste que les contrôles sont conçus de manière appropriée pour répondre aux critères retenus.

Les critères couverts par la démarche CaliaLabs incluent : sécurité (protection contre l'accès non autorisé), disponibilité (résilience et continuité), confidentialité (protection des données sensibles), intégrité du traitement (exactitude et complétude), vie privée (conforme au RGPD).

L'évaluation est confiée à un cabinet d'audit indépendant enregistré auprès de l'AICPA. Les contrôles évalués portent sur : l'infrastructure (accès physique et logique, segmentation réseau, chiffrement), la gestion des identités et des accès (MFA, revues périodiques, provisioning/déprovisioning), la surveillance et la détection (journaux d'événements, alertes, réponse aux incidents), la gestion des changements (revue de code, tests, déploiements contrôlés).

Date cible : achèvement au troisième trimestre 2026. Le rapport final sera mis à disposition des clients sous accord de confidentialité.

3. SOC 2 Type II — Quatrième trimestre 2026

SOC 2 Type II prolonge le Type I en évaluant non seulement la conception des contrôles, mais aussi leur efficacité opérationnelle sur une période d'observation de plusieurs mois (généralement 6 à 12 mois).

La période d'observation démarre immédiatement après l'obtention du Type I. Pendant cette période, l'auditeur collecte des preuves de l'exécution continue des contrôles : échantillons de journaux, enregistrements d'alertes traitées, comptes-rendus de revues périodiques, preuves de tests de reprise d'activité, et historique des incidents.

Date cible : achèvement au quatrième trimestre 2026. Ce jalon représente un engagement significatif en matière de maturité opérationnelle, au-delà de la simple existence théorique des contrôles.

4. ISO/IEC 27001 — Quatrième trimestre 2026

ISO/IEC 27001 est la norme internationale de référence en matière de système de management de la sécurité de l'information (SMSI). Elle couvre l'ensemble des pratiques de gestion des risques et de protection de l'information.

La démarche CaliaLabs vise la certification selon la version ISO/IEC 27001:2022, qui intègre les évolutions récentes en matière de menaces numériques, de conformité aux réglementations territoriales, et d'intégration avec les autres référentiels (27017 pour le cloud, 27018 pour les données personnelles).

Les domaines couverts incluent : politique de sécurité, organisation de la sécurité, gestion des actifs, sécurité des ressources humaines, contrôle d'accès, cryptographie, sécurité physique, sécurité des opérations, sécurité des commu-

nications, acquisition et maintenance des systèmes, relations fournisseurs, gestion des incidents, continuité d'activité, conformité.

Date cible : certification initiale au quatrième trimestre 2026, avec audits de surveillance annuels prévus pour les trois années suivantes.

5. DORA — Alignement Article 30

Le Règlement (UE) 2022/2554 relatif à la résilience opérationnelle numérique du secteur financier (DORA) est entré en pleine application le 17 janvier 2025. Il impose aux entités financières et à leurs prestataires critiques un ensemble d'exigences en matière de gestion des risques liés aux technologies de l'information et de la communication.

L'Article 30 définit le contenu minimum obligatoire des contrats entre entités financières et prestataires TIC tiers. CaliaLabs s'est assuré que ses contrats-types et ses pratiques opérationnelles permettent à ses clients financiers de répondre à l'intégralité des dispositions de cet article.

Les éléments couverts incluent notamment : description précise des services fournis et des niveaux de service, localisation du traitement et du stockage des données, obligations de notification en cas d'incident, droits d'audit et d'accès aux informations, plans de sortie et de réversibilité, conditions de sous-traitance et transparence sur la chaîne de fournisseurs, clauses de résiliation en cas de défaillance grave.

Le Data Processing Agreement (DPA) et le Service Level Agreement (SLA) publiés dans ce Trust Center formalisent ces engagements.

6. RGPD — Conformité native

Le Règlement général sur la protection des données (RGPD) est respecté de manière native par l'infrastructure CEREBRO : minimisation des données collectées, finalités explicites et limitées, durées de conservation définies par politique, séparation stricte des rôles responsable de traitement / sous-traitant, droits des personnes (accès, rectification, effacement, portabilité, opposition) exercés via des procédures formalisées.

La documentation détaillée est disponible dans le Data Processing Agreement (DPA), la Politique de Confidentialité, et la Politique de Conservation des Données, toutes accessibles depuis le Trust Center.

7. Gouvernance de la démarche

L'ensemble des démarches de certification est piloté par l'équipe conformité de CaliaLabs, sous la responsabilité du dirigeant. Les partenaires externes (auditeurs, conseils) sont sélectionnés pour leur indépendance, leur connaissance du secteur financier, et leur capacité à évaluer des architectures techniques complexes.

Les jalons sont suivis en interne via un tableau de bord dédié, avec reporting mensuel à la direction. Les écarts éventuels par rapport au calendrier sont documentés avec leurs causes et les actions correctives associées.

Ce document est mis à jour à chaque franchissement de jalon significatif, ou au minimum chaque trimestre.

8. Contact

Pour toute question relative à la démarche de conformité ou à l'obtention d'un rapport d'audit sous accord de confidentialité, l'équipe dédiée est joignable à compliance@calialabs.com.

Les demandes d'information émanant d'auditeurs externes ou d'autorités de régulation sont traitées en priorité, avec une première réponse sous 48 heures ouvrées.