NANOGUARD

Audit RC Pro, Cyber et RGPD pour sociétés IA

CONFIDENTIEL — NANOGUARD 2025

DOSSIER EXÉCUTIF D'EXPOSITION AU RISQUE

Rapport d'Audit RC/Cyber

Évaluation structurée des expositions RC Pro, cyber et protection des données afin d'orienter les décisions d'assurance, de conformité et de remédiation prioritaire.

Société auditée

FinFlux

DATE D'ÉMISSION

26 avril 2026

Ce rapport synthétise les signaux les plus critiques observés et propose une trajectoire d'assainissement priorisée, compatible avec un usage PDF client.

Score global et cadrage métier

Vue d'ensemble de l'exposition actuelle de l'entreprise, destinée à situer immédiatement le niveau d'urgence et le contexte opérationnel de l'audit.

RÉFÉRENCE DOSSIER · FINFLUX

Score de risque global

64 /100

MODÉRÉ

FAIBLE | MODÉRÉ | ÉLEVÉ | CRITIQUE

Niveau observé: Modéré

Score déclaré: 64/100

Secteur

Fintech / scoring de crédit IA

Type d'activité

Plateforme SaaS d'analyse de solvabilité et d'octroi de crédit assisté par IA pour établissements financiers

Lecture opérationnelle

La combinaison du secteur, de la nature des traitements et du score global permet de calibrer les priorités d'assurance, les exigences de sécurité et le niveau de formalisation attendu côté conformité.

Signal principal

Modéré

Exposition dominante à surveiller de près avant évolution du volume de clients, de données ou d'usage.

Décision recommandée

Prioriser les mesures à impact rapide

Les pages suivantes détaillent les risques les plus sensibles et la séquence d'action recommandée.

Expositions en responsabilité civile professionnelle

Cette page recense les scénarios dans lesquels une défaillance produit, une erreur de recommandation ou un dommage causé à un tiers peut déclencher une mise en cause contractuelle ou extracontractuelle.

MATRICE RC PRO

Axes d'analyse

L'objectif est d'identifier les points où la promesse commerciale, l'automatisation et la dépendance opérationnelle du client créent un risque de préjudice mesurable.

- Erreur ou dérive de recommandation impactant un client final
- Défaut de supervision humaine sur une décision sensible
- Promesse marketing non alignée avec les limites réelles du produit
- Insuffisance de traçabilité lors d'un litige ou d'une réclamation

Bloc compatible avec 4 scénarios RC Pro priorisés pour FinFlux

Risques identifiés

Défaut de résultat sur un usage métier critique

ÉLEVÉ

Une automatisation mal supervisée peut produire une erreur de traitement ou une recommandation erronée causant un dommage économique à un client.

Impact estimé: Réclamation client et perte commerciale

Promesse produit trop large

MODÉRÉ

Une communication commerciale plus ambitieuse que les garanties réelles du produit fragilise la défendabilité du prestataire en cas de litige.

Impact estimé: Contentieux contractuel

Absence de supervision humaine sur cas sensibles

ÉLEVÉ

Sans point de contrôle humain sur les décisions sensibles, l'entreprise augmente son exposition RC et ses difficultés de justification post-incident.

Impact estimé: Préjudice tiers et mise en cause

Journalisation insuffisante des arbitrages

MODÉRÉ

En cas de contestation, l'absence d'historique fiable sur les actions, validations et limites de service affaiblit le dossier.

Impact estimé: Charge probatoire élevée

Surface d'attaque numérique et posture de conformité

Cette synthèse combine les principaux scénarios cyber, la maturité de gouvernance des données et les mesures immédiates attendues pour réduire l'exposition réglementaire.

CYBER / DONNÉES PERSONNELLES

Risques cyber identifiés

Compromission d'un compte administrateur

ÉLEVÉ

Un compte à privilèges compromis peut exposer les données clients, les intégrations et la configuration opérationnelle du service.

Impact estimé

Accès étendu aux données et réglages

Mauvaise séparation multi-tenant

ÉLEVÉ

Une isolation incomplète entre environnements ou comptes clients augmente le risque de fuite, d'altération ou de confusion de données.

Impact estimé

Fuite inter-clients

Rétention excessive de données

MODÉRÉ

Conserver plus de données ou plus longtemps que nécessaire augmente l'impact potentiel d'un incident et la charge de conformité.

Impact estimé

Sur-exposition réglementaire

Chaîne d'intégration insuffisamment contrôlée

MODÉRÉ

Les API, webhooks et accès prestataires étendent la surface d'attaque si les secrets, journaux et limitations d'usage ne sont pas maîtrisés.

Impact estimé

Propagation d'incident

Bloc compatible avec 4 scénarios cyber priorisés pour FinFlux

CONFORMITÉ RGPD

Exposition modérée à élevée: gouvernance et documentation à consolider.

État synthétique de la gouvernance des données, de la base légale, de la documentation et des mesures de sécurité attendues pour les traitements concernés.

Recommandations immédiates

1. Encadrer les cas d'usage sensibles avec validation humaine, contrat de service clair et journalisation des décisions.
2. Renforcer les contrôles d'accès, la séparation des environnements et la revue des privilèges.
3. Documenter la gouvernance des données, les durées de conservation et les bases légales applicables.

Priorités de remédiation recommandées

Les actions ci-dessous sont ordonnées pour réduire rapidement le risque résiduel, renforcer la posture assurantielle et améliorer la défendabilité du dossier client.

FEUILLE DE ROUTE 30-90 JOURS

Plan d'action prioritaire

PRIORITÉ	ACTION	PILOTE	DÉLAI
P1	**Cartographier les usages et engagements sensibles** Identifier les parcours où une erreur produit un dommage mesurable et aligner la promesse commerciale sur les limites réelles du produit.	Direction produit	15 jours
P1	**Durcir les accès privilégiés** Imposer MFA, moindre privilège, revue d'accès et séparation claire entre rôles internes, support et client.	Responsable sécurité	30 jours
P2	**Renforcer l'isolation des données** Vérifier la séparation logique des tenants, l'étanchéité des exports et les contrôles sur les environnements de test.	Engineering	30 jours
P2	**Mettre à jour la documentation RGPD** Compléter registre, DPA, politique de conservation, documentation sécurité et procédures de notification d'incident.	Juridique / DPO	45 jours
P3	**Préparer un dossier de preuve client** Constituer les journaux d'arbitrage, la matrice de risques et les métriques de qualité pour défendre le service en cas de contestation.	Ops / Sales	60 jours

Bloc compatible avec 5 actions ordonnées sur 60 jours

Synthèse exécutive et prochaines étapes

La conclusion rappelle le niveau de vigilance requis, reformule l'orientation de traitement et prépare la prise de contact avec NanoGuard pour la suite du dossier.

CLÔTURE DU RAPPORT

Résumé exécutif

FinFlux présente un profil modéré avec un score de 64/100, principalement lié à son activité de plateforme saas d'analyse de solvabilité et d'octroi de crédit assisté par ia pour établissements financiers dans le secteur fintech / scoring de crédit ia. L'analyse repose sur les informations déclaratives disponibles pour FinFlux. Les priorités portent sur la gouvernance des opérations, l'encadrement contractuel et le cloisonnement technique des accès, données et infrastructures exposées.

Prochaines étapes recommandées

Valider sous 30 jours les actions P1, cadrer la gouvernance des usages sensibles avec les parties prenantes métier et préparer un point de suivi NanoGuard afin de mesurer la baisse de risque résiduel après remédiation.

Contact NanoGuard

Pour approfondir ce rapport, cadrer les actions correctives ou préparer la mise en place d'une couverture adaptée, contacter directement l'équipe NanoGuard.

INTERLOCUTEUR

NanoGuard

EMAIL

nanoguard@nanocorp.app

TÉLÉPHONE

Sur demande