P R O B E

AUDIT TECHNIQUE · CONFIDENTIEL

Audit technique de *Acme Inc.*

Un état des lieux indépendant, des risques hiérarchisés, des recommandations actionnables.

COMMANDITAIRE Contoso Capital	CIBLE AUDITÉE Acme Inc.	AUTEUR Jonathan Brossard
PÉRIMÈTRE Plateforme SaaS	DATE DE REMISE 09/04/2026	VERSION V1.2
RÉFÉRENCE PROBE-2026-017	CLASSIFICATION Confidentiel	DIFFUSION Commanditaire

PAGES LIMINAIRES

Versions, contacts et diffusion

Historique des versions

VERSION	DATE	AUTEUR	MODIFICATIONS
V1.0	24/03/2026	Jonathan Brossard	Rédaction initiale. Transmise à l'éditeur pour procédure contradictoire.
V1.1	31/03/2026	Jonathan Brossard	Intégration de la réponse de l'éditeur. Portée du constat DAT-02 révisée à la baisse après examen des éléments produits. État de traitement porté sur chaque constat.
V1.2	09/04/2026	Jonathan Brossard	Vérification des correctifs livrés par l'éditeur entre le 26/03 et le 02/04. Calendrier d'engagement consolidé. Annexes A à I mises à jour.

Contacts

CONTOSO CAPITAL — COMMANDITAIRE

NOM	RÔLE	TÉLÉPHONE	COURRIEL
Nicolas S.	Partner	+33 X XX XX XX XX	nicolas@example.com

ACME INC. — CIBLE AUDITÉE

NOM	RÔLE	TÉLÉPHONE	COURRIEL
Jacques M.	Directeur général	+33 X XX XX XX XX	jacques@example.com
Sophie R.	Responsable technique	+33 X XX XX XX XX	sophie@example.com

PROBE — AUDITEUR

NOM	RÔLE	TÉLÉPHONE	COURRIEL
Jonathan Brossard	Fondateur	+33 X XX XX XX XX	contact@probe-audit.fr

DIFFUSION

Ce rapport est établi pour le seul usage de Contoso Capital, dans le cadre défini par la lettre de mission du 24 février 2026 et par l'accord de confidentialité tripartite du 20 février 2026. Il ne peut être communiqué qu'intégralement, aux conseils et financeurs de Contoso Capital intervenant sur l'opération. Toute autre diffusion, ainsi que la diffusion d'un extrait isolé, requiert l'accord écrit préalable de Probe.

Une déclaration d'indépendance et d'absence de conflit d'intérêts figure en annexe I. Elle fait partie intégrante du présent rapport.

SOMMAIRE

Sommaire

SECTION 1

Synthèse exécutive

Cet audit est conduit pour Contoso Capital, dans la perspective d'une prise de participation majoritaire au capital d'Acme Inc, éditeur d'une plateforme SaaS de planification d'interventions terrain. Il porte sur la plateforme elle-même — code, données, exploitation — et intervient à un moment charnière : le plan d'affaires prévoit de multiplier par quatre la base clients en trois ans, sur une architecture qui n'a pas encore été éprouvée à cette échelle.

L'audit répond à trois questions distinctes.

La plateforme est-elle bien conçue ? Oui dans ses fondations : le choix d'un monolithe modulaire TypeScript, la cohérence du modèle de données et la discipline de versionnement témoignent d'une équipe qui sait ce qu'elle fait.

Est-elle bien exploitée ? Non, à ce stade : la supervision ne couvre que l'infrastructure, aucune procédure d'incident n'est écrite, et la capacité de restauration n'a jamais été démontrée.

Est-elle reprenable ? Partiellement : la documentation est suffisante pour l'essentiel, mais le module de facturation — celui dont les erreurs coûtent le plus cher — repose sur la connaissance d'une seule personne.

Quatre constats structurent cette appréciation.

Le cloisonnement des données entre clients repose exclusivement sur la couche applicative. Aucun mécanisme de cloisonnement n'existe au niveau de la base : l'isolation entre les 42 clients dépend d'un filtre appliqué dans le code d'accès aux données. Ce filtre est correctement implémenté dans les 340 requêtes examinées, mais rien n'empêche structurellement qu'une nouvelle requête l'omette. Un correctif partiel a été livré pendant la procédure contradictoire — activation de la *Row Level Security* sur les six tables portant des données nominatives ; les vingt-trois autres tables restent exposées au même mécanisme.

La capacité à restaurer les sauvegardes n'a jamais été vérifiée. Les sauvegardes automatiques sont bien configurées et leur exécution est journalisée, mais aucune restauration n'a été réalisée depuis la mise en production du cluster actuel, il y a quatorze mois. L'éditeur ne dispose donc d'aucune mesure de son délai de reprise réel, ni de la preuve que ses sauvegardes sont exploitables — alors qu'il contractualise un objectif de reprise de quatre heures.

La couverture de tests est absente sur le module de facturation. La couverture globale s'établit à 31 %, ce qui est faible sans être disqualifiant. Elle tombe à 4 % sur le module de facturation — précisément celui dont les erreurs sont les plus coûteuses à détecter tardivement, et celui qui concentre la connaissance d'un seul ingénieur.

Le coût d'infrastructure croît plus vite que la base clients. Sur les dix-huit derniers mois, le nombre de clients a progressé de 61 % et la facture d'infrastructure de 143 %. L'écart ne s'explique pas par la volumétrie mais par deux choix réversibles : un surdimensionnement de l'instance de base de données et l'absence de tout cache applicatif. À trajectoire inchangée, le coût par client augmente au lieu de diminuer.

En conséquence, l'audit recommande de traiter trois points sans délai :

1. **Étendre le cloisonnement au niveau base à l'ensemble des tables multi-clients.** Motif : c'est le seul constat dont la réalisation aurait des conséquences contractuelles et réglementaires immédiates. *Partiellement traité au 28/03/2026.*

2. **Retirer les secrets de l'historique du dépôt d'infrastructure et faire tourner les identifiants concernés.** Motif : trois identifiants de service restent lisibles dans l'historique git, dont un toujours valide à l'ouverture de la mission. *Partiellement traité au 26/03/2026.*
3. **Réaliser et documenter une restauration complète en environnement isolé.** Motif : sans cette mesure, l'engagement de service pris auprès des clients n'est pas étayé. *Ouvert, engagé pour le 30/04/2026.*

1.1 Opinion de l'auditeur

OPINION

Les investigations menées permettent de conclure que la plateforme d'Acme Inc est techniquement saine dans sa conception et opérationnellement immature dans son exploitation. Aucun constat ne remet en cause la viabilité du produit ni la compétence de l'équipe qui le développe. Deux réserves se dégagent, d'importance inégale : l'une porte sur un risque de réalisation à court terme, l'autre sur le coût des évolutions futures. La première est traitable en quelques semaines ; la seconde conditionne la trajectoire à trois ans.

Première réserve — l'exploitation n'est pas outillée à la hauteur de l'engagement pris. Ce n'est pas un constat isolé mais le mécanisme commun à trois d'entre eux : l'absence de restauration éprouvée (EXP-01), une supervision aveugle au métier et aux traitements planifiés (EXP-02) et l'absence de toute procédure d'incident écrite (EXP-03) relèvent du même angle mort. L'équipe sait construire, elle n'a pas encore appris à surveiller. Cette réserve comptera davantage demain qu'aujourd'hui : à 42 clients, un incident se détecte par l'appel d'un client mécontent ; à 170, ce mode de détection n'est plus tenable, et l'engagement de disponibilité contractualisé devient un passif.

Seconde réserve — la maintenabilité est inégale, et l'inégalité porte sur le mauvais module. Il faut distinguer ici ce qui dégrade le produit livré de ce qui détermine le coût des évolutions. Rien dans les constats ne dégrade le produit tel que l'utilisateur le reçoit : les performances sont correctes aux volumes actuels et aucun défaut fonctionnel n'a été relevé. En revanche, la conjonction d'une couverture de tests quasi nulle et d'une concentration de connaissance sur le module de facturation crée une zone où chaque évolution future sera lente, risquée et dépendante d'une personne. C'est cette zone qui déterminera le coût réel de la feuille de route, pas l'architecture d'ensemble.

En conséquence, Probe considère que le risque technique associé à la plateforme Acme est **maîtrisable**, sous réserve du traitement des trois points de phase 1 avant closing — 11 à 14 jours-homme — et de l'inscription au budget post-opération d'un chantier d'industrialisation de l'exploitation et de la couverture de tests, chiffré à **33 jours-homme** (détail au §8.1).

SECTION 2

Contexte et périmètre

2.1 Contexte

Acme Inc édite depuis 2020 une plateforme SaaS de planification d'interventions terrain, destinée aux entreprises de maintenance multi-sites. Elle est utilisée par 42 clients représentant environ 11 000 utilisateurs nommés, dont 2 300 techniciens en mobilité. Le développement est assuré en interne par une équipe de sept ingénieurs, sans recours à la sous-traitance.

Le produit est en croissance et la société envisage une opération capitalistique destinée à financer son expansion. L'audit vise à apprécier le risque technique attaché à la plateforme : ce que le système peut porter, ce qu'il coûtera à maintenir, et les dépendances susceptibles d'en compromettre la continuité.

L'audit est strictement technique. Il ne comprend ni appréciation de la valeur de la société, ni audit financier ou comptable, ni qualification juridique, ni évaluation du positionnement commercial du produit.

2.2 Calendrier de la mission

DATE	PHASE	CONTENU
24/02/2026	Cadrage	Lettre de mission signée. Définition du périmètre avec le commanditaire, identification des points de vigilance issus du plan d'affaires, liste des accès à ouvrir.
27/02 → 02/03	Ouverture des accès	Accès en lecture seule aux deux dépôts et à la console d'infrastructure. Une copie restaurée de la base de production, datée du 10/03/2026, a été mise à disposition en cours d'analyse.
02/03 → 20/03	Analyse	Reconstruction de l'environnement de référence, revue du code et de l'infrastructure, mesures, onze entretiens avec l'équipe technique et la direction.
24/03/2026	Remise V1.0	Rapport transmis au commanditaire et, pour procédure contradictoire, à l'éditeur.
26/03/2026	Restitution	Présentation orale au commanditaire et à ses conseils, puis session de questions.
31/03/2026	Contradictoire	Réponse écrite de l'éditeur (onze pages). Publication de la V1.1.
09/04/2026	Remise V1.2	Vérification des correctifs livrés, consolidation du calendrier d'engagement. Version définitive.

Durée totale : six semaines du cadrage à la version définitive, dont dix-huit jours d'analyse effective.

2.3 Périmètre technique

L'audit porte sur la branche `main` du dépôt principal, au commit `4f1a2c9` du 12 mars 2026, et sur le dépôt d'infrastructure au commit `e83b501` de la même date. Le dépôt principal totalise 187 000 lignes de TypeScript, 4 100 commits et 61 migrations de schéma depuis l'origine. L'historique est continu depuis la création du projet.

Trois ensembles sont couverts :

- **L'application** — monolithe modulaire NestJS 10 / TypeScript 5.3, déployé en conteneurs sur AWS ECS Fargate en région `eu-west-1`, derrière un répartiteur de charge applicatif. Onze modules fonctionnels, dont planification, mobilité, facturation et référentiel clients.
- **La base de données** — PostgreSQL 15 sur RDS, instance `db.r6g.2xlarge` en configuration multi-AZ. 29 tables, dont 6 portant des données nominatives. 34 index, aucune politique de sécurité au niveau ligne au commit audité.
- **Les chaînes d'intégration** — ingestion de fichiers clients par dépôt S3 (7 formats propriétaires), envoi de notifications par un service Node séparé s'appuyant sur SES et sur un fournisseur SMS tiers, et 14 tâches planifiées exécutées par EventBridge.

2.4 Nature des informations analysées

ÉLÉMENT ANALYSÉ	SOURCE PRINCIPALE	NIVEAU D'ASSURANCE
Cloisonnement des données entre clients	Preuve directe — lecture des 340 requêtes du module d'accès, catalogue `pg_policies`	Élevé
Volumétrie, index, plans d'exécution	Mesure sur copie restaurée de production	Élevé
Couverture de tests et complexité	Mesure — exécution de la chaîne d'intégration sur le commit audité	Élevé
Répartition de la connaissance dans l'équipe	Mesure — analyse de l'historique git par module	Élevé
Secrets présents dans l'historique	Preuve directe — parcours de l'historique des deux dépôts	Élevé
Exposition réseau et surface d'attaque	Analyse de configuration, non validée par test d'intrusion	Moyen
Coûts d'infrastructure et leur trajectoire	Factures fournisseur communiquées par l'éditeur	Moyen
Délais de détection des incidents passés	Registre d'incidents de l'éditeur, recoupé avec deux échanges clients	Moyen
Procédures de sauvegarde et de reprise	Document interne de l'éditeur, non éprouvé	Déclaratif
Engagements de disponibilité contractuels	Document interne de l'éditeur	Déclaratif
Résistance à une attaque	—	Non vérifié
Comportement sous charge nominale ×4	—	Non vérifié

2.5 Évolution du code depuis le commit audité

Le rapport a été transmis à l'éditeur le 24 mars 2026. Entre le commit audité (`4f1a2c9`, 12 mars) et le commit de référence de la présente version (`9d7e1b4`, 2 avril), **63 commits** ont été poussés sur `main`.

Quatre évolutions comptent pour la lecture du rapport : l'activation de la Row Level Security sur les six tables nominatives, la mise en place d'une expiration des jetons d'API, l'ajout des deux index manquants sur le chemin critique de planification, et la pseudonymisation de l'environnement de préproduction.

Les mesures de la section 7 restent établies au commit audité ; chaque constat de la section 6 porte son état de traitement individuel, avec sa date, le commit correspondant et le niveau de vérification de la correction.

SECTION 3

Axes d'analyse

Six domaines structurent l'analyse. Ils correspondent exactement aux familles de codes utilisées pour les constats en section 6, dans le même ordre — de sorte qu'un constat se situe sans ambiguïté dans le plan du rapport.

CODE	DOMAINE	CE QUI EST EXAMINÉ	SECTION
SEC	Sécurité applicative & cloisonnement	Authentification, gestion des secrets, isolation entre clients, surface d'exposition	6.1
DAT	Modèle de données & couche d'accès	Schéma, migrations, indexation, motifs d'accès, plans d'exécution	6.2
EXP	Exploitation, supervision & continuité	Sauvegardes et reprise, supervision, alertes, gestion des incidents	6.3
MNT	Maintenabilité, qualité & capacité de reprise	Couverture de tests, complexité, dépendances, documentation, répartition de la connaissance	6.4
RGP	Données à caractère personnel	Assiette des données nominatives, environnements, durées de conservation	6.5
ARC	Architecture d'exploitation, montée en charge & coûts	Dimensionnement, mise en cache, trajectoire de coûts, capacité à absorber la croissance	6.6

Le tableau de maturité du §7.1 utilise une grille plus fine — huit domaines pondérés — dont la correspondance avec ces six familles est indiquée en tête de tableau.

SECTION 4

Limites de la mission

L'audit s'appuie sur le code source et son historique complet, sur la configuration d'infrastructure versionnée, sur une copie restaurée de la base de production datée du 10 mars 2026, sur les factures fournisseur des dix-huit derniers mois, sur la documentation interne communiquée, et sur onze entretiens conduits avec l'équipe technique et la direction.

La mission ne comprend pas :

- **de test d'intrusion** : l'audit vérifie la présence et la portée des protections, non leur résistance à une attaque ;
- **de test de charge** : aucune donnée de volumétrie, de temps de réponse ou de concurrence n'a été produite sous charge simulée. Les constats relatifs à la montée en charge reposent sur l'analyse des plans d'exécution et de l'architecture, non sur une mesure ;
- **de qualification juridique des constats relatifs aux données à caractère personnel**, qui relève du délégué à la protection des données du commanditaire ;
- **de revue du code du service de notifications**, hébergé dans un dépôt distinct auquel l'accès n'a pas été ouvert. Son interface avec la plateforme a été examinée, son implémentation non ;
- **d'appréciation de la propriété intellectuelle** sur les composants développés, ni de vérification de la conformité des licences des dépendances tierces au-delà de leur inventaire ;
- **d'audit des tiers** : les fournisseurs d'hébergement, d'identité et d'envoi de messages sont pris comme des dépendances dont la configuration est examinée, non comme des systèmes audités.

> PORTÉE D'UNE OBLIGATION DE MOYENS
>
> Les conclusions du présent rapport reposent sur les éléments mis à disposition et sur les déclarations recueillies, dans les limites du temps imparti. Elles ne constituent ni une certification, ni une garantie d'exhaustivité, ni une garantie quant à l'absence de défauts ou de vulnérabilités non détectés. Les niveaux d'assurance du §2.4 indiquent, pour chaque catégorie d'information, le degré de vérification atteint.

SECTION 5

Méthodologie

5.1 Approche générale

Démarche en trois temps : reconstruction d'un environnement de référence, collecte et vérification, puis synthèse et hiérarchisation des risques. La démarche privilégie la preuve sur la déduction ; les constats reposant sur la seule analyse statique sont signalés comme tels.

5.2 Environnement de référence

Un environnement fonctionnel a été reconstruit à partir des seuls éléments versionnés dans les deux dépôts, sans assistance de l'équipe. Cette contrainte est délibérée : elle mesure la capacité de reprise autant qu'elle sert l'analyse. Le démarrage a nécessité trois interventions non documentées, relevées au constat MNT-04. Procédure complète en annexe B.

5.3 Méthode d'évaluation

Chaque constat est qualifié selon deux dimensions.

DIMENSION	ÉCHELLE ET SIGNIFICATION
Gravité	**Critique** : conséquence immédiate et difficilement réversible si le risque se matérialise · **Élevée** : conséquence sérieuse, réversible au prix d'un effort · **Moyenne** : effet différé ou circonscrit · **Faible** : effet marginal à l'échelle actuelle
Portée	**Isolée** : se corrige en un point du système · **Intermédiaire** : touche plusieurs composants ou processus · **Structurelle** : relève d'un choix de conception ou d'organisation, et se paie sur toute la durée de vie du produit

La portée est déterminante : un défaut grave mais circonscrit se corrige, un défaut moyen mais structurel se paie durablement. C'est pourquoi la matrice du §7.2 croise les deux dimensions plutôt que de produire un classement unique.

Chaque constat porte également son **niveau de preuve** — établi par preuve directe, mesuré, ou déclaratif — et son **état de traitement** :

ÉTAT	SIGNIFICATION
Corrigé	Correctif livré et vérifié par l'auditeur
Partiel	Correctif livré sur une partie du périmètre, reste documenté
Ouvert	Aucun correctif livré à la date de remise
Arbitré	L'éditeur a écarté tout ou partie de la recommandation, arbitrage documenté
Clos	Constat sans objet après examen des éléments produits

Tout état est assorti de sa date, du commit correspondant et du niveau de vérification. **Aucun constat n'est retiré du rapport** : un constat corrigé y demeure, avec la trace de sa correction.

5.4 Agrégation des constats en risques

La section 7 regroupe les constats en risques lorsqu'ils concourent au même effet. Deux règles gouvernent ce regroupement :

1. Un risque agrégé **hérite de la gravité et de la portée maximales** des constats qui le composent. Un risque regroupant un constat critique structurel et deux constats élevés intermédiaires est donc positionné en critique structurel.
2. Un constat peut alimenter **un seul** risque, afin que la somme des risques couvre exactement l'ensemble des constats, sans double compte ni omission.

Ces règles rendent le passage des quatorze constats aux sept risques entièrement reconstituable par le lecteur.

5.5 Traçabilité

Chaque constat est rattaché à un emplacement précis dans le code (`chemin/fichier:ligne`), à une mesure reproductible ou à une requête. Aucun constat n'est formulé sans élément permettant au lecteur de le vérifier lui-même. Les annexes A à F rassemblent ces éléments par catégorie de preuve.

5.6 Procédure contradictoire

Le rapport a été transmis à l'éditeur le 24 mars 2026. L'éditeur a répondu le 31 mars par un document de onze pages, contestant **un constat sur quatorze** — DAT-02, dont la portée a été révisée à la baisse après examen des éléments produits — et proposant un calendrier de traitement pour les autres.

La présente version intègre ces éléments ainsi que la vérification des correctifs livrés entre le 26 mars et le 2 avril. La procédure contradictoire n'a pas pour objet d'atténuer les constats, mais de séparer ce qui est établi de ce qui reposait sur une lecture incomplète, et de donner au commanditaire l'état réel du système à la date de sa décision.

SECTION 6

Constats et analyse

Quatorze constats sont formulés, répartis sur les six domaines du §3. Chacun porte sa gravité, sa portée, son niveau de preuve, l'élément qui l'établit, une recommandation chiffrée et son état de traitement à la date de remise.

6.1 Sécurité applicative & cloisonnement

L'appréciation d'ensemble est mitigée. Les fondamentaux sont en place et correctement implémentés : authentification déléguée à un fournisseur d'identité éprouvé, mots de passe non stockés, chiffrement en transit et au repos, absence de dépendance vulnérable connue au commit audité. La lecture des 340 requêtes du module d'accès aux données n'a révélé *aucune* omission du filtre de cloisonnement, ce qui atteste d'une véritable discipline d'équipe.

Les réserves ne portent donc pas sur ce qui a été fait, mais sur ce qui ne dépend que de la vigilance humaine et pourrait être garanti structurellement.

SEC-01 — Cloisonnement multi-clients garanti par la seule couche applicative

GRAVITÉ : CRITIQUE | PORTÉE : STRUCTURELLE | ÉTABLI PAR PREUVE DIRECTE

L'isolation des données entre les 42 clients repose exclusivement sur un filtre `tenant_id` appliqué dans le module d'accès aux données. Au commit audité, aucune politique de sécurité au niveau ligne n'est définie dans la base : le catalogue `pg_policies` est vide, et `pg_class.relrowsecurity` est faux sur les 29 tables.

Ce filtre est correctement appliqué partout où il devait l'être. Le constat ne porte pas sur un défaut existant mais sur l'absence de garde-fou : toute requête écrite hors du module d'accès, tout accès direct par un outil d'administration et toute erreur d'un nouvel arrivant produirait une fuite inter-clients sans qu'aucune barrière ne s'y oppose. Le mécanisme est le même que celui du constat RGP-01.

Ce constat n'implique *pas* qu'une fuite se soit produite : aucune trace de ce type n'a été relevée dans les journaux d'accès des quatre-vingt-dix derniers jours.

> CONCRÈTEMENT
>
> ```
> -- Au commit 4f1a2c9, sur copie restaurée du 10/03/2026 : 0 ligne
> SELECT schemaname, tablename, policyname FROM pg_policies;
>
> -- 29 tables, toutes à relrowsecurity = false
> SELECT relname, relrowsecurity FROM pg_class
>  WHERE relnamespace = 'public'::regnamespace AND relkind = 'r';
> ```
>
> Filtre applicatif : `src/core/data/tenant-scope.guard.ts:47`
>
> Chemins contournant le module d'accès : `src/modules/reporting/exports.service.ts:112` et `:189` — deux requêtes brutes, filtre présent mais écrit à la main.

RECOMMANDATION — activer la Row Level Security sur l'ensemble des 29 tables portant une colonne `tenant_id`, avec une politique dérivée du contexte de session ; adjoindre un test de non-régression échouant si une table multi-clients est créée sans politique. **Effort estimé : 6 à 9 jours-homme**, dont 2 pour les deux requêtes brutes de `exports.service.ts`. Script de vérification en annexe A.

Partiel

le 28/03/2026 (`b12f4a8`) — RLS activée sur les 6 tables nominatives, vérifié sur le dépôt et en production. 23 tables restent sans politique. Engagement éditeur : phase 2, échéance 30/05/2026.

SEC-02 — Jetons d'API clients sans expiration ni rotation

GRAVITÉ : ÉLEVÉE | PORTÉE : ISOLÉE | ÉTABLI PAR PREUVE DIRECTE

Les 61 jetons d'API délivrés aux clients pour leurs intégrations sont émis sans date d'expiration et sans mécanisme de rotation. Le plus ancien jeton actif au commit audité avait été émis 38 mois plus tôt. Aucune procédure de révocation en cas de départ d'un salarié côté client n'existe, et le client ne dispose d'aucun moyen autonome de faire tourner son jeton.

La portée est isolée : le défaut se corrige sans toucher à l'architecture, et le périmètre de chaque jeton est correctement restreint au client émetteur.

> CONCRÈTEMENT
>
> ```
> SELECT count(*), min(created_at) FROM api_tokens WHERE revoked_at IS NULL;
> --  61 | 2023-01-17
> SELECT count(*) FROM api_tokens WHERE expires_at IS NOT NULL;
> --   0
> ```
>
> Émission : `src/modules/auth/api-token.service.ts:34` — le champ `expires_at` existe au schéma et n'est jamais alimenté.

RECOMMANDATION — fixer une durée de validité de douze mois, notifier le client trente jours avant échéance, exposer la rotation en libre-service. **Effort estimé : 3 jours-homme.**

Corrigé

le 30/03/2026 (`7c4d012`) — expiration à 12 mois, rotation en libre-service, notification à J-30. Vérifié en production sur un jeton de test.

SEC-03 — Identifiants de service lisibles dans l'historique du dépôt d'infrastructure

GRAVITÉ : ÉLEVÉE | PORTÉE : INTERMÉDIAIRE | ÉTABLI PAR PREUVE DIRECTE

Trois identifiants de service figurent en clair dans l'historique du dépôt d'infrastructure, introduits entre juin 2021 et février 2023 puis retirés des fichiers courants sans réécriture de l'historique. À l'ouverture de la mission, l'un des trois — la clé du fournisseur SMS — était **toujours valide**.

Le dépôt est privé et l'accès restreint à sept personnes, ce qui contient l'exposition. Elle n'est pas nulle pour autant : un accès en lecture accordé temporairement, un clone local sur un poste non chiffré ou une sauvegarde de poste suffisent à la matérialiser. Un secret présent dans un historique git doit être considéré comme diffusé, non comme supprimé.

CONCRÈTEMENT

```
git log -p --all -S'SMS_API_KEY=' -- terraform/env/prod.tfvars
# introduit en 3a91f7c (2021-06-14), retiré en d02e5b1 (2023-02-09)
```

Les deux autres : clé de service S3 (`3a91f7c`), mot de passe de l'ancien cluster RDS (`88b2e40`, ressource détruite depuis).

RECOMMANDATION — faire tourner immédiatement la clé SMS, réécrire l'historique ou considérer les trois secrets comme durablement compromis, et ajouter une détection de secrets en pré-commit. **Effort estimé : 2 jours-homme.**

Partiel

le 26/03/2026 (`a55f918`) — clé SMS révoquée et remplacée, vérifié auprès du fournisseur. Détection pré-commit en place. Historique non réécrit : arbitrage éditeur assumé, les deux secrets restants portant sur des ressources détruites.

6.2 Modèle de données & couche d'accès

Le modèle est cohérent, normalisé et lisible. Les 61 migrations sont réversibles et exécutées en intégration continue à chaque publication. Les réserves portent sur l'indexation du chemin critique et sur un motif d'accès, non sur la conception.

DAT-01 — Absence d'index sur deux colonnes de jointure du chemin critique

GRAVITÉ : MOYENNE | PORTÉE : INTERMÉDIAIRE | MESURÉ

Deux colonnes de jointure du chemin de planification — l'écran le plus consulté du produit — ne sont pas indexées, produisant des parcours séquentiels sur les deux tables les plus volumineuses. Aux volumes actuels le temps de réponse reste acceptable ; il croît linéairement avec la volumétrie, laquelle croît avec le nombre de clients.

CONCRÈTEMENT

```
EXPLAIN (ANALYZE, BUFFERS)
SELECT ... FROM interventions i
  JOIN technician_slots s ON s.intervention_id = i.id ...;

-- Seq Scan on technician_slots (1 840 220 lignes) ... 412 ms
-- Seq Scan on interventions    (  611 480 lignes) ... 187 ms
-- Total : 684 ms
```

Après ajout des deux index : **31 ms**, soit un facteur 22. Requête et mesures rejouables en annexe F.

RECOMMANDATION — créer les deux index en `CONCURRENTLY`. **Effort estimé : 0,5 jour-homme.**

Corrigé

le 27/03/2026 (`f4e8b23`) — deux index créés, mesure de confirmation à 34 ms en production.

DAT-02 — Requêtes en cascade sur l'écran de planning hebdomadaire

GRAVITÉ : MOYENNE | PORTÉE : ISOLÉE | MESURÉ

Le chargement du planning hebdomadaire déclenche 1 + n requêtes, où n est le nombre de techniciens affichés. Pour un client de 90 techniciens, l'affichage produit 91 requêtes et 1,4 seconde de temps serveur.

Portée révisée après procédure contradictoire : initialement qualifiée d'intermédiaire, ramenée à isolée après production par l'éditeur de la démonstration que le module de planification est le seul à présenter ce motif d'accès.

> CONCRÈTEMENT
>
> `src/modules/scheduling/weekly-view.service.ts:88` — boucle appelant `slotRepository.findByTechnician()` à chaque itération. Trace des 91 requêtes reproductible en activant `DEBUG=orm:query` sur le scénario décrit en annexe F.

RECOMMANDATION — remplacer la boucle par une requête agrégée unique. **Effort estimé : 2 jours-homme.**

Ouvert *phase 2 — engagement éditeur : échéance 30/05/2026.*

6.3 Exploitation, supervision & continuité

C'est le domaine le plus faible de l'audit, et le seul où les constats se renforcent mutuellement : la même défaillance n'est ni prévenue, ni détectée, ni outillée. Les trois constats qui suivent forment le risque R2 et le risque R5.

EXP-01 — Capacité de restauration jamais éprouvée

GRAVITÉ : ÉLEVÉE | PORTÉE : STRUCTURELLE | DÉCLARATIF

Les sauvegardes automatiques RDS sont configurées avec une rétention de sept jours et leur exécution est journalisée sans échec sur la période observée. Aucune restauration n'a cependant été réalisée depuis la mise en service du cluster actuel, quatorze mois plus tôt.

L'éditeur ne dispose donc d'aucune mesure de son délai de reprise réel. Le contrat-cadre signé avec ses clients énonce un objectif de reprise de quatre heures : cet engagement n'est étayé par aucune mesure, et la première restauration se ferait en situation d'incident, sous pression, sans procédure écrite.

Ce constat est classé déclaratif : il repose sur les déclarations concordantes de l'équipe et sur l'absence de toute trace de restauration, non sur une preuve positive.

> CONCRÈTEMENT
>
> ```
> aws cloudtrail lookup-events \
>   --lookup-attributes AttributeKey=EventName,\
> AttributeValue=RestoreDBInstanceFromDBSnapshot
> # aucun événement sur la période de rétention des journaux
> ```
>
> Aucune procédure de restauration dans la documentation interne communiquée. Confirmé en entretien par la responsable technique le 18/03/2026.

RECOMMANDATION — réaliser une restauration complète en environnement isolé, chronométrer chaque étape, en tirer une procédure écrite, et réitérer semestriellement. **Effort estimé : 3 jours-homme** pour le premier exercice, puis 0,5 par itération.

Ouvert *phase 1 — engagement éditeur : premier exercice avant le 30/04/2026.*

EXP-02 — Supervision limitée à l'infrastructure, aucune alerte métier

GRAVITÉ : MOYENNE | PORTÉE : STRUCTURELLE | ÉTABLI PAR PREUVE DIRECTE

Les 14 alertes configurées portent toutes sur des métriques d'infrastructure : processeur, mémoire, espace disque, santé des cibles du répartiteur. Aucune ne porte sur un indicateur métier. En particulier, l'échec de l'une des 14 tâches planifiées — dont l'ingestion quotidienne des fichiers clients et la génération des factures mensuelles — ne déclenche aucune notification.

Conséquence pratique : un échec silencieux d'ingestion est détecté par le client, pas par l'équipe. Deux incidents de ce type figurent au registre des douze derniers mois, avec des délais de détection de 19 et 31 heures.

> CONCRÈTEMENT
>
> ```
> aws cloudwatch describe-alarms \
>   --query 'MetricAlarms[].[AlarmName,Namespace]'
> # 14 alarmes — namespaces AWS/ECS, AWS/RDS, AWS/ApplicationELB
> # aucune métrique applicative personnalisée
> ```
>
> Tâches planifiées : `infra/eventbridge/schedules.tf` — 14 règles, aucune cible de gestion d'échec, aucune file d'attente de messages non traités.

RECOMMANDATION — instrumenter les 14 tâches planifiées avec une alerte sur absence de terminaison réussie, et ajouter quatre indicateurs métier : volume d'ingestion, taux d'erreur d'envoi, factures générées, sessions actives. **Effort estimé : 5 jours-homme.**

Ouvert

phase 2 — engagement éditeur : échéance 30/06/2026.

EXP-03 — Aucune procédure de gestion d'incident écrite

GRAVITÉ : MOYENNE | PORTÉE : STRUCTURELLE | DÉCLARATIF

Aucun document ne décrit qui est joignable en cas d'incident majeur, dans quel ordre, ni selon quels critères un client est informé. Il n'existe pas d'astreinte formalisée, pas de canal dédié, et pas de gabarit de communication client. Le registre d'incidents est tenu *a posteriori*, sans analyse de cause racine et sans suivi des actions correctives.

Les deux incidents d'ingestion mentionnés en EXP-02 illustrent l'effet combiné : ni détection outillée, ni chaîne d'escalade. À 42 clients, la connaissance implicite de l'équipe compense ; à 170, elle ne compensera plus, et l'engagement de reprise de quatre heures suppose une chaîne de décision qui n'existe pas sur le papier.

> CONCRÈTEMENT
>
> Documentation interne communiquée : 4 documents, dont aucun ne décrit la conduite à tenir pendant un incident — le seul document s'y rapportant est le registre, tenu après les faits. Registre d'incidents : 7 entrées sur 12 mois, comportant une date et une description, sans cause racine, sans action corrective, sans délai de détection renseigné — les délais de 19 et 31 heures ont été reconstitués par recoupement avec deux échanges clients.
>
> Confirmé en entretien : l'escalade repose sur l'appel direct de la responsable technique, sans suppléant désigné.

RECOMMANDATION — rédiger une procédure d'incident de deux pages : critères de gravité, chaîne d'appel avec suppléant, seuil d'information client, gabarit de communication. Étendre le registre à la cause racine et au suivi des actions. **Effort estimé : 2 jours-homme.**

Ouvert

phase 2 — porté au calendrier d'engagement par l'audit ; l'éditeur n'avait pas identifié ce point.

6.4 Maintenabilité, qualité & capacité de reprise

Le code est lisible, les conventions sont tenues et la chaîne d'intégration est fiable. Les réserves ne portent pas sur le niveau moyen mais sur sa *dispersion* : la partie la moins testée et la moins partagée du code est aussi celle dont les erreurs coûtent le plus cher.

MNT-01 — Concentration de la connaissance sur le module de facturation

GRAVITÉ : MOYENNE | PORTÉE : STRUCTURELLE | MESURÉ

Un ingénieur est l'auteur de 68 % des commits du module de facturation sur les vingt-quatre derniers mois, et de 91 % de ceux touchant le calcul des prorata. Aucun autre membre de l'équipe n'a modifié ce dernier fichier depuis dix-sept mois.

Le module concerné est celui dont les erreurs sont les plus coûteuses — une erreur de facturation se découvre chez le client — et celui dont la couverture de tests est la plus faible (MNT-02). Ces trois faits pris ensemble constituent le risque R4.

CONCRÈTEMENT

```
git shortlog -sn --since='24 months ago' -- src/modules/billing/
#  214  ingénieur A   (68 %)
#   61  ingénieur B
#   39  autres (4 personnes)

git log -1 --format=%ad -- src/modules/billing/proration.calculator.ts
# dernière modification par un autre auteur : il y a 17 mois
```

RECOMMANDATION — revue croisée obligatoire sur le module, documentation des règles de calcul, et reprise progressive par un second ingénieur. **Effort estimé : 8 jours-homme** répartis sur un trimestre, dont 4 pour la revue croisée et la documentation.

Arbitré

le 31/03/2026 — l'éditeur retient la revue croisée et la documentation (4 j-h), et écarte la reprise par un second ingénieur avant le second semestre, pour cause de charge de feuille de route. Arbitrage documenté ; le risque R4 est maintenu en l'état et le commanditaire est invité à l'intégrer à son plan post-opération.

MNT-02 — Couverture de tests quasi nulle sur le module de facturation

GRAVITÉ : MOYENNE | PORTÉE : STRUCTURELLE | MESURÉ

La couverture de tests globale s'établit à 31 % en lignes. Elle est très inégalement répartie : 74 % sur le module de planification, 4 % sur celui de facturation. Le calcul des prorata, 310 lignes portant l'essentiel de la complexité métier, n'est couvert par aucun test.

Une couverture de 31 % n'est pas disqualifiante en soi pour un produit de cet âge. Ce qui l'est davantage, c'est que la partie non couverte soit celle dont une régression se découvre sur une facture client, un mois après la mise en production.

> CONCRÈTEMENT
>
> ```
> npm run test:coverage    # commit 4f1a2c9
> All files                 31,4 %
>  modules/scheduling       74,2 %
>  modules/billing           4,1 %
>   proration.calculator     0,0 %   (310 lignes, complexité cyclomatique 47)
> ```
>
> Détail par fichier et complexité des vingt fichiers les plus complexes en annexe F.

RECOMMANDATION — couvrir en priorité le calcul des prorata par des tests fondés sur des cas réels anonymisés, cible de 70 % sur le module. **Effort estimé : 12 jours-homme.**

Ouvert — *phase 3 — engagement éditeur : intention pour le second semestre 2026, sans échéance ferme.*

MNT-03 — Dépendance non maintenue sur le parseur de fichiers clients

GRAVITÉ : FAIBLE | PORTÉE : ISOLÉE | ÉTABLI PAR PREUVE DIRECTE

Le parseur utilisé pour les sept formats d'ingestion clients n'a reçu aucune publication depuis 37 mois et son dépôt amont est archivé. Aucune vulnérabilité connue ne l'affecte à ce jour. La bibliothèque est utilisée en 4 emplacements et son interface est étroite.

Le constat est classé faible délibérément : remplacer une dépendance qui fonctionne, sans vulnérabilité et sans blocage fonctionnel, est un mauvais emploi du temps d'ingénierie. Ce qui doit être fait maintenant, c'est rendre le remplacement futur trivial.

> CONCRÈTEMENT
>
> `package.json:41` — dernière version publiée il y a 37 mois, dépôt amont archivé par son auteur. Usages : `src/modules/ingestion/parsers/*.ts` (4 fichiers).

RECOMMANDATION — encapsuler derrière une interface interne pour rendre le remplacement trivial le jour où il s'imposera. Ne pas remplacer tant que rien ne l'impose. **Effort estimé : 2 jours-homme.**

Ouvert — *phase 3 — sans urgence.*

MNT-04 — Trois étapes de démarrage non documentées

GRAVITÉ : FAIBLE | PORTÉE : ISOLÉE | ÉTABLI PAR PREUVE DIRECTE

La reconstruction de l'environnement à partir des seuls éléments versionnés a nécessité trois interventions absentes de la documentation : création manuelle d'un rôle base, variable d'environnement non listée, et amorçage d'une table de référence. Un nouvel arrivant perd une demi-journée sur ces trois points, et un repreneur davantage.

> CONCRÈTEMENT
>
> Procédure complète en 14 étapes, y compris les trois écarts relevés, en annexe B.

RECOMMANDATION — compléter le `README` et ajouter un script d'amorçage exécutable. **Effort estimé : 1 jour-homme.**

Corrigé — *le 02/04/2026 (`9d7e1b4`) — vérifié par reconstruction complète depuis le dépôt, sans aucune intervention manuelle.*

6.5 Données à caractère personnel

Un seul constat, mais il commande le risque R1 conjointement avec SEC-01. La qualification juridique des faits relevés ici relève du délégué à la protection des données du commanditaire, non de l'auditeur : le constat est technique.

RGP-01 — Données de production utilisées en préproduction sans pseudonymisation

GRAVITÉ : ÉLEVÉE | PORTÉE : INTERMÉDIAIRE | ÉTABLI PAR PREUVE DIRECTE

L'environnement de préproduction est alimenté par une copie hebdomadaire de la base de production, sans pseudonymisation. Il contient donc les données nominatives des 11 000 utilisateurs — noms, adresses électroniques professionnelles — et les coordonnées de géolocalisation des 2 300 techniciens. L'accès à cet environnement est ouvert aux sept membres de l'équipe technique, contre trois en production.

Le constat technique est double : l'assiette des données nominatives est plus large que nécessaire, et son accès est plus permissif que celui de la production qu'elle copie.

> CONCRÈTEMENT
>
> ```
> infra/scripts/refresh-staging.sh:22
> # pg_dump intégral suivi d'un pg_restore, aucune transformation
> ```
>
> Comptage sur la copie du 10/03 : 11 042 lignes nominatives dans `users`, 2 314 positions dans `technician_positions`.

RECOMMANDATION — insérer une étape de pseudonymisation dans le script de rafraîchissement, et aligner les droits d'accès sur ceux de la production. **Effort estimé : 4 jours-homme.**

Corrigé — *le 29/03/2026 (`c81a3f7`) — pseudonymisation des noms, adresses et positions, vérifiée par échantillonnage sur la copie du 01/04. Alignement des droits d'accès également effectué.*

6.6 Architecture d'exploitation, montée en charge & coûts

Un constat unique, mais c'est celui qui a l'effet financier le plus directement chiffrable — et le seul entièrement réversible.

ARC-01 — Coût d'infrastructure croissant plus vite que la base clients

GRAVITÉ : MOYENNE | PORTÉE : INTERMÉDIAIRE | MESURÉ

Sur dix-huit mois, le nombre de clients a progressé de 61 % et le coût mensuel d'infrastructure de 143 %. L'écart n'est pas imputable à la volumétrie mais à deux choix réversibles : l'instance de base de données est dimensionnée à `db.r6g.2xlarge` pour une utilisation processeur moyenne de 11 % et une pointe à 34 %, et aucun cache applicatif n'est en place, ce qui reporte sur la base l'intégralité des lectures répétées.

À trajectoire inchangée et au volume prévu par le plan d'affaires, le coût par client augmente au lieu de décroître — l'inverse de ce qu'on attend d'un modèle SaaS à cette étape, et une hypothèse qui pèse directement sur la marge brute projetée.

> CONCRÈTEMENT
>
> Factures fournisseur (source déclarative) : 4 180 €/mois en septembre 2024 pour 26 clients, soit 161 € par client ; 10 160 €/mois en février 2026 pour 42 clients, soit 242 € par client.
>
> Utilisation RDS mesurée sur 90 jours : moyenne 11 %, p95 22 %, pointe 34 %. Détail en annexe F.

RECOMMANDATION — redimensionner à `db.r6g.large` après validation sur la pointe réelle, et introduire un cache sur les trois lectures les plus fréquentes. **Effort estimé : 6 jours-homme**, pour une économie estimée de 3 200 à 3 800 €/mois, soit 38 000 à 46 000 € par an.

Ouvert

phase 3 — engagement éditeur : intention pour le second semestre 2026, sans échéance ferme. Le redimensionnement suppose au préalable le test de charge recommandé au §8.

> RÉCAPITULATIF DES ÉTATS À LA DATE DE REMISE
>
> **Corrigé et vérifié (4)** : SEC-02, DAT-01, MNT-04, RGP-01 — **Partiel (2)** : SEC-01, SEC-03 — **Arbitré (1)** : MNT-01 — **Ouvert (7)** : DAT-02, EXP-01, EXP-02, EXP-03, MNT-02, MNT-03, ARC-01. Total : quatorze constats.

SECTION 7

Évaluation des risques

Les quatorze constats sont regroupés en sept risques, selon les règles d'agrégation du §5.4 : chaque risque hérite de la gravité et de la portée maximales de ses constats, et chaque constat alimente un seul risque. La somme des sept risques couvre donc exactement l'ensemble des constats.

RISQUE CRITIQUE

R1 — Fuite de données entre clients (SEC-01, RGP-01) — l'isolation entre les 42 clients ne dépend d'aucune barrière structurelle, et l'assiette des données nominatives dépasse celle de la production. Une erreur d'implémentation unique, non détectable par la revue actuelle, suffirait à matérialiser le risque, avec des conséquences contractuelles et réglementaires immédiates.
État V1.2 : partiellement traité — barrière posée sur les six tables nominatives et préproduction pseudonymisée ; 23 tables demeurent sans politique.

RISQUES ÉLEVÉS

R2 — Incapacité à reprendre après un sinistre dans le délai contractualisé (EXP-01) — l'engagement de reprise en quatre heures n'est étayé par aucune mesure, et la première restauration se ferait en situation d'incident.
État V1.2 : ouvert — exercice engagé pour avril 2026.

R3 — Persistance d'accès non maîtrisés (SEC-02, SEC-03) — jetons clients actifs jusqu'à 38 mois sans révocation possible côté client, et secrets de service lisibles dans un historique git.
État V1.2 : partiellement traité — jetons corrigés, clé SMS révoquée, historique non réécrit par arbitrage assumé.

RISQUES MOYENS

R4 — Dépendance à une personne sur le module de facturation (MNT-01, MNT-02) — la conjonction d'une concentration de connaissance à 68 % et d'une couverture de tests à 4 % rend chaque évolution de ce module lente, risquée et non délégable. C'est le risque qui pèsera le plus sur le coût de la feuille de route.
État V1.2 : arbitré — revue croisée et documentation retenues, reprise par un second ingénieur écartée jusqu'au S2 2026.

R5 — Cécité opérationnelle (EXP-02, EXP-03) — les défaillances des traitements planifiés sont détectées par les clients, avec des délais mesurés de 19 et 31 heures, et aucune chaîne d'escalade n'est écrite. Tenable à 42 clients, intenable à 170.
État V1.2 : ouvert.

R6 — Dégradation du rendement à la montée en charge (DAT-01, DAT-02, ARC-01) — les trois constats concourent au même effet : un coût unitaire et des temps de réponse qui se dégradent avec la croissance plutôt que de s'améliorer. Aucun n'est structurel individuellement.
État V1.2 : partiellement traité — indexation corrigée ; cascade de requêtes et dimensionnement ouverts.

RISQUE FAIBLE

R7 — Obsolescence de composants et lacunes de documentation (MNT-03, MNT-04) — dépendance archivée sans vulnérabilité connue, et écarts de documentation de démarrage.
État V1.2 : partiellement traité — documentation corrigée ; encapsulation du parseur ouverte, sans urgence.

La hiérarchie implique un séquencement clair. R1, R2 et R3 relèvent du **risque de réalisation** : leur matérialisation aurait un effet immédiat, et ils doivent être refermés avant closing. R4 et R6 relèvent du **coût de détention** : ils ne menacent rien à court terme mais déterminent le budget des trois prochaines années, et se traitent au plan post-opération. R5 se situe entre les deux : sans urgence aujourd'hui, il devient un risque élevé au franchissement du seuil de croissance prévu au plan d'affaires.

7.1 Tableau de maturité technique

Huit domaines notés sur 5 et pondérés. Cette grille est plus fine que les six familles de constats du §3 : la colonne « Famille » indique la correspondance. La note globale est la moyenne pondérée ; **elle ne se substitue pas à l'analyse détaillée**.

DOMAINE	FAMILLE	POND.	NOTE	COMMENTAIRE
Architecture & conception	DAT / ARC	15 %	3,5 / 5	Monolithe modulaire cohérent, frontières nettes entre modules, choix assumés et documentés
Modèle de données & couche d'accès	DAT	15 %	3,0 / 5	Schéma normalisé et migrations réversibles ; indexation du chemin critique incomplète au commit audité
Sécurité applicative & cloisonnement	SEC	25 %	2,5 / 5	Fondamentaux en place et discipline réelle, mais aucune garantie structurelle du cloisonnement
Exploitation & supervision	EXP	15 %	2,0 / 5	Sauvegardes configurées mais jamais éprouvées, supervision aveugle au métier, aucune procédure d'incident
Qualité & tests	MNT	10 %	2,5 / 5	Chaîne d'intégration en place et fiable ; couverture inégale, absente là où elle importe le plus
Maintenabilité & capacité de reprise	MNT	10 %	3,0 / 5	Code lisible et conventions tenues ; concentration de connaissance sur un module critique
Documentation & transmissibilité	MNT	5 %	2,0 / 5	Documentation d'architecture correcte, documentation opérationnelle absente

DOMAINE	FAMILLE	POND.	NOTE	COMMENTAIRE
Gouvernance technique, dépendances & coûts	ARC / MNT	5 %	3,0 / 5	Dépendances à jour à une exception près ; trajectoire de coûts non pilotée
Maturité globale		**100 %**	**5,4 / 10**	**Plateforme saine dans sa conception, immature dans son exploitation**

Moyenne pondérée : 2,70 sur 5, rapportée sur 10. Notes établies au commit audité `4f1a2c9`, avant les correctifs de la procédure contradictoire.

Lecture de la note

Une maturité de 5,4 traduit une plateforme qui fonctionne, tenue par une équipe compétente, et qui n'a pas encore franchi l'étape d'industrialisation. Elle ne traduit *pas* un risque de défaillance à court terme : aucun constat n'indique une instabilité du produit livré. Elle traduit en revanche que la croissance prévue par le plan d'affaires exigera un investissement d'industrialisation qui n'est pas aujourd'hui inscrit au budget.

Une note comparable se rencontre couramment chez un éditeur de cette taille au même stade. Ce qui distingue les trajectoires ensuite, c'est le traitement du domaine « Exploitation » — le plus faible ici, et le moins coûteux à redresser.

7.2 Matrice de synthèse des risques

	ISOLÉE	INTERMÉDIAIRE	STRUCTURELLE
CRITIQUE	—	—	**R1** Fuite inter-clients
ÉLEVÉE	—	**R3** Accès non maîtrisés	**R2** Reprise après sinistre
MOYENNE	—	**R6** Rendement à la montée en charge	**R4** Dépendance personne clé **R5** Cécité opérationnelle
FAIBLE	**R7** Obsolescence & documentation	—	—

Lecture : la colonne de droite relève du plan d'action immédiat pour les risques critique et élevés, du traitement planifié pour les moyens ; la colonne centrale du traitement planifié ; la colonne de gauche de l'amélioration continue. Aucun risque de gravité critique ou élevée n'est de portée isolée : aucun ne se corrige par un correctif ponctuel unique.

SECTION 8

Recommandations et plan d'action

Phase 1 — Immédiatement, avant closing

1. **Étendre la Row Level Security aux 23 tables restantes** et adjoindre le test de non-régression (SEC-01). 6 à 9 jours-homme. *Partiellement traité.*
2. **Réécrire l'historique du dépôt d'infrastructure** ou acter formellement la compromission durable des deux secrets restants (SEC-03). 2 jours-homme. *Partiellement traité.*
3. **Réaliser et documenter une restauration complète chronométrée** en environnement isolé (EXP-01). 3 jours-homme. *Ouvert, engagé pour avril.*

Phase 2 — Dans les semaines qui suivent

1. **Instrumenter les 14 tâches planifiées et ajouter quatre indicateurs métier** (EXP-02). 5 jours-homme. Meilleur rapport effort / réduction de risque de tout le plan.
2. **Rédiger la procédure de gestion d'incident** et étendre le registre à la cause racine (EXP-03). 2 jours-homme.
3. **Supprimer la cascade de requêtes du planning hebdomadaire** (DAT-02). 2 jours-homme.
4. **Mettre en place la revue croisée et la documentation du module de facturation** (MNT-01, volet retenu par l'éditeur). 4 jours-homme.

Phase 3 — Sur le trimestre

1. **Porter la couverture de tests du module de facturation à 70 %** (MNT-02). 12 jours-homme.
2. **Redimensionner la base et introduire un cache applicatif** (ARC-01, §6.6). 6 jours-homme, pour une économie estimée de 38 000 à 46 000 € par an.
3. **Encapsuler le parseur d'ingestion derrière une interface interne** (MNT-03). 2 jours-homme.

Hors périmètre du présent audit

1. **Conduire un test de charge à quatre fois le volume actuel**, afin de valider les hypothèses de dimensionnement du §6.6. 5 jours-homme. Cette mesure conditionne le redimensionnement recommandé en phase 3 : sans elle, la pointe réelle reste une hypothèse.

Le séquencement suit un ordre délibéré : d'abord **ce qui expose** — le cloisonnement et les secrets, dont la matérialisation aurait des conséquences immédiates et irréversibles ; puis **ce qui aveugle** — la restauration non éprouvée, la supervision et l'absence de procédure d'incident, qui déterminent la capacité à réagir ; ensuite **ce qui alourdit** — la couverture de tests et la concentration de connaissance, qui grèvent chaque évolution future ; enfin **ce qui coûtera** — la trajectoire d'infrastructure, dont l'effet est réel mais différé et parfaitement réversible.

8.1 Chiffrage consolidé

PÉRIMÈTRE	CONSTATS CONCERNÉS	JOURS-HOMME
Phase 1 — avant closing	SEC-01, SEC-03, EXP-01	11 à 14

PÉRIMÈTRE	CONSTATS CONCERNÉS	JOURS-HOMME
Phase 2 — semaines suivantes	EXP-02, EXP-03, DAT-02, MNT-01	13
Phase 3 — sur le trimestre	MNT-02, ARC-01, MNT-03	20
Total des correctifs restants		**44 à 47**
Dont chantier d'industrialisation post-opération (phases 2 et 3)		33
Correctifs déjà livrés et vérifiés	SEC-02, DAT-01, MNT-04, RGP-01	8,5
Hors périmètre — test de charge	—	5

Les chiffrages sont exprimés en jours-homme d'un ingénieur familier du code et n'incluent ni la revue, ni la recette, ni la coordination. Un jour-homme n'est pas un jour calendaire.

Un point d'attention pour le commanditaire : les 4 jours-homme écartés par l'éditeur sur MNT-01 — la reprise du module de facturation par un second ingénieur — ne figurent pas au total ci-dessus. Ils resteront à financer, avant ou après l'opération.

8.2 Calendrier d'engagement de l'éditeur

ÉCHÉANCE	ENGAGEMENT	ÉTAT AU 09/04/2026
30/04/2026	Premier exercice de restauration documenté (EXP-01)	Engagé
30/05/2026	RLS sur les 23 tables restantes (SEC-01)	Engagé
30/05/2026	Suppression de la cascade de requêtes (DAT-02)	Engagé
30/06/2026	Supervision métier et alertes sur tâches planifiées (EXP-02)	Engagé
30/06/2026	Revue croisée et documentation du module de facturation (MNT-01)	Engagé
S2 2026	Couverture de tests facturation, redimensionnement (MNT-02, ARC-01)	Intention, sans échéance ferme
—	Reprise du module facturation par un second ingénieur (MNT-01)	Écarté — arbitrage assumé

Trois points ne figuraient pas au calendrier proposé par l'éditeur. L'audit les y ajoute, sans engagement de sa part à ce jour :

ÉCHÉANCE	POINT AJOUTÉ PAR L'AUDIT	ÉTAT AU 09/04/2026
Phase 2	Procédure de gestion d'incident et extension du registre (EXP-03)	Porté par l'audit — non engagé
Phase 1	Réécriture de l'historique du dépôt d'infrastructure (SEC-03)	Porté par l'audit — écarté par l'éditeur
Préalable à la phase 3	Test de charge à quatre fois le volume actuel (hors périmètre)	Porté par l'audit — non engagé

Le dernier des trois conditionne le redimensionnement recommandé : sans mesure sous charge, les hypothèses de dimensionnement resteront non validées au moment où elles compteront.

CONCLUSION

Conclusion

La plateforme d'Acme Inc est techniquement saine dans sa conception et immature dans son exploitation. L'équipe de sept ingénieurs qui la développe fait preuve d'une discipline réelle — 340 requêtes examinées sans une seule omission du filtre de cloisonnement en témoigne mieux que n'importe quelle déclaration. Ce qui manque n'est pas la compétence, c'est l'outillage que la croissance rendra indispensable.

Les investissements identifiés, ordonnés selon la logique du plan d'action :

1. **Ce qui expose** — l'absence de garantie structurelle du cloisonnement inter-clients et les secrets résiduels dans l'historique (SEC-01, SEC-03) : **8 à 11 jours-homme**.
2. **Ce qui aveugle** — la restauration jamais éprouvée, la supervision aveugle au métier et l'absence de procédure d'incident (EXP-01 à EXP-03) : **10 jours-homme**.
3. **Ce qui alourdit** — la couverture de tests du module de facturation, la concentration de connaissance qui l'accompagne et l'encapsulation du parseur (MNT-01 à MNT-03) : **18 jours-homme**, plus un arbitrage organisationnel que l'audit ne peut trancher à la place de la direction.
4. **Ce qui coûtera** — la trajectoire d'infrastructure, à 242 € par client et croissante, et le motif d'accès du planning (ARC-01, DAT-02) : **8 jours-homme** pour une économie annuelle de 38 000 à 46 000 €.

Soit **44 à 47 jours-homme** de correctifs restants, auxquels s'ajoutent 5 jours pour le test de charge recommandé hors périmètre, et 8,5 jours déjà consommés par l'éditeur sur les correctifs livrés pendant la procédure contradictoire.

> BILAN DES CONSTATS AU 09/04/2026
>
> **Quatorze constats** : 4 corrigés et vérifiés, 2 partiellement traités, 1 arbitré, 7 ouverts dont 3 engagés sous échéance ferme. Aucun constat n'a été retiré au cours de la procédure contradictoire ; un seul — DAT-02 — a vu sa portée révisée à la baisse sur production d'éléments par l'éditeur.

Sous réserve du traitement des trois points de phase 1 avant closing, et de l'inscription au budget post-opération d'un chantier d'industrialisation de 33 jours-homme, **aucun obstacle technique significatif à l'opération envisagée n'a été identifié**.

ANNEXES

Annexes

Une annexe par catégorie de preuve, afin que tout constat soit vérifiable sans interroger l'auditeur. Les annexes font partie intégrante du rapport.

Annexe A — Commandes de vérification en production

Requêtes et appels permettant au commanditaire de vérifier lui-même l'état des correctifs, sans accès privilégié ni assistance de l'éditeur.

SEC-01 — CLOISONNEMENT AU NIVEAU BASE

```
-- Doit retourner 29 lignes distinctes une fois SEC-01 clos
SELECT tablename, policyname FROM pg_policies ORDER BY 1;

-- Doit retourner 0 ligne : aucune table multi-clients sans RLS
SELECT c.relname FROM pg_class c
  JOIN pg_attribute a ON a.attrelid = c.oid
 WHERE a.attname = 'tenant_id'
   AND c.relkind = 'r' AND NOT c.relrowsecurity;
```

SEC-02 — EXPIRATION DES JETONS

```
-- Doit retourner 0 : plus aucun jeton actif sans expiration
SELECT count(*) FROM api_tokens
 WHERE revoked_at IS NULL AND expires_at IS NULL;
```

DAT-01 — INDEXATION DU CHEMIN CRITIQUE

```
-- Doit lister les deux index créés le 27/03
SELECT indexname FROM pg_indexes
 WHERE tablename IN ('technician_slots','interventions')
   AND indexdef LIKE '%intervention_id%';
```

RGP-01 — PSEUDONYMISATION DE LA PRÉPRODUCTION

```
-- Sur l'environnement de préproduction : doit retourner 0
SELECT count(*) FROM users
 WHERE email NOT LIKE '%@example.invalid';
```

Annexe B — Reproduire l'environnement d'audit

Procédure complète en 14 étapes, du clone au jeu de données de référence, telle qu'exécutée pour la mission — y compris les trois écarts relevés au constat MNT-04 et depuis corrigés : création du rôle `app_readonly`, variable `INGEST_BUCKET_REGION` absente du fichier d'exemple, et amorçage de la table `reference_skills`.

Mesures de référence rejouables sur cet environnement, destinées à établir l'avancement des correctifs :

MESURE	AU COMMIT AUDITÉ	CIBLE
Temps de réponse du planning hebdomadaire (90 techniciens)	1 400 ms	< 300 ms
Requête de jointure du chemin critique	684 ms	< 50 ms
Couverture de tests — module facturation	4,1 %	70 %
Couverture de tests — globale	31,4 %	50 %
Tables multi-clients sans politique RLS	29	0
Durée du démarrage à froid depuis un clone	4 h 10	< 1 h

Annexe C — Éléments de preuve des constats critiques

SEC-01 — extrait du catalogue `pg_policies` avant et après correctif ; liste des 340 requêtes du module d'accès avec, pour chacune, la présence constatée du filtre `tenant_id` ; les deux requêtes brutes de `exports.service.ts` reproduites intégralement avec leur contexte d'appel ; extrait des journaux d'accès des 90 derniers jours établissant l'absence de trace de fuite.

SEC-03 — commits d'introduction et de retrait des trois secrets, avec empreintes tronquées permettant l'identification sans reproduire les valeurs ; confirmation écrite de révocation obtenue du fournisseur SMS le 26/03/2026 ; configuration de la détection pré-commit installée.

RGP-01 — comptages nominatifs sur la copie du 10/03 et sur celle du 01/04, établissant l'effet de la pseudonymisation ; comparaison des listes de droits d'accès production / préproduction avant et après alignement.

Annexe D — Correctifs livrés avec le rapport

Probe livre avec le présent rapport les éléments suivants, utilisables tels quels par l'éditeur et vérifiables par le commanditaire :

- Migration d'activation de la Row Level Security pour les 23 tables restantes, avec politique dérivée du contexte de session et rollback.
- Test de non-régression échouant sur toute table portant `tenant_id` et dépourvue de politique, intégrable à la chaîne d'intégration existante.
- Script de pseudonymisation de la préproduction, appelé depuis `refresh-staging.sh`.
- Gabarit de procédure de gestion d'incident (EXP-03), à compléter par l'éditeur.

Ces éléments sont fournis à titre d'accélérateur. Leur intégration, leur recette et leur exploitation demeurent de la responsabilité de l'éditeur, et les jours-homme du §8.1 en tiennent compte.

Annexe E — État des correctifs des audits antérieurs

Trois sujets avaient été relevés par l'audit interne de mai 2025. Leur état a été vérifié dans le cadre de la présente mission :

SUJET	CORRECTION APPORTÉE	ÉTAT
Rotation des clés de chiffrement	Rotation annuelle automatisée, dernière exécution vérifiée en janvier 2026	Corrigé
Séparation des environnements	Comptes distincts production / préproduction, plus aucun accès croisé	Corrigé
Journalisation des accès administrateur	Journalisation active en production uniquement ; la préproduction en est dépourvue	Partiel

Le caractère partiel du troisième point recoupe le constat RGP-01 : jusqu'au 29/03/2026, l'environnement le moins journalisé était aussi celui qui contenait le plus de données nominatives.

Annexe F — Détail des mesures

- Couverture de tests par fichier, pour les onze modules fonctionnels.
- Complexité cyclomatique des vingt fichiers les plus complexes, dont `proration.calculator.ts` (310 lignes, complexité 47).
- Plans d'exécution avant et après indexation, avec `BUFFERS` et temps d'exécution sur trois exécutions consécutives.
- Comptages de volumétrie par table sur la copie du 10/03/2026.
- Utilisation processeur, mémoire et connexions de l'instance RDS sur 90 jours : moyenne, p95, pointe, avec horodatage de la pointe.
- Trace des 91 requêtes du planning hebdomadaire pour un client de 90 techniciens.
- Répartition des commits par module et par auteur sur 24 mois.

Annexe G — Sources analysées

NATURE	ÉLÉMENTS
Code source	Deux dépôts aux commits `4f1a2c9` et `e83b501`, historique git complet depuis 2020
Données	Copie restaurée de la base de production du 10/03/2026, en environnement isolé
Infrastructure	Configuration Terraform versionnée, consoles AWS en lecture seule, journaux CloudTrail et CloudWatch
Documents de l'éditeur	4 documents internes : architecture, procédure de sauvegarde, contrat-cadre client, registre d'incidents
Éléments financiers	18 mois de factures du fournisseur d'hébergement
Entretiens	11 entretiens : direction générale (2), responsable technique (3), ingénieurs (5), support (1)

NATURE	ÉLÉMENTS
Procédure contradictoire	Document de réponse de l'éditeur du 31/03/2026 (11 pages) et ses annexes

Annexe H — Glossaire

Chaque terme technique employé dans le rapport, défini pour un lecteur non technique.

TERME	DÉFINITION
Row Level Security (RLS)	Mécanisme de la base de données qui filtre les lignes visibles selon le contexte de la connexion. Contrairement à un filtre écrit dans le code, il s'applique quelle que soit la requête : c'est une barrière et non une convention.
Parcours séquentiel	Lecture de toutes les lignes d'une table faute d'index utilisable. Le temps de réponse croît alors proportionnellement au volume de données.
Requêtes en cascade	Motif où l'affichage d'une liste de n éléments déclenche n requêtes supplémentaires au lieu d'une seule requête agrégée. Invisible en développement, coûteux en production.
Complexité cyclomatique	Nombre de chemins d'exécution possibles dans une fonction. Au-delà de 15, une fonction devient difficile à tester exhaustivement ; à 47, elle l'est en pratique impossible sans tests écrits.
Couverture de tests	Proportion des lignes de code exécutées lors du passage de la suite de tests. Une couverture élevée ne garantit pas l'absence de défaut ; une couverture nulle garantit qu'aucune régression ne sera détectée automatiquement.
Multi-AZ	Configuration où la base de données est répliquée dans deux centres de données distincts d'une même région, permettant un basculement automatique en cas de panne de l'un des deux.
Délai de reprise (RTO)	Temps écoulé entre un sinistre et le retour au service. Il ne se déduit pas de la configuration des sauvegardes : il se mesure en réalisant une restauration.
Pseudonymisation	Remplacement des données identifiantes par des valeurs artificielles, de sorte qu'un environnement de test reste exploitable sans exposer de personnes réelles.
Monolithe modulaire	Application déployée en un seul bloc, mais organisée en modules aux frontières explicites. Combine la simplicité d'exploitation du monolithe et une partie de la souplesse d'évolution des microservices.
Dette technique	Écart entre l'état du code et celui qu'exigerait son niveau d'usage. Elle ne se rembourse pas nécessairement : elle se chiffre, et l'on décide de la porter ou de la réduire.

Annexe I — Déclaration d'indépendance et d'absence de conflit d'intérêts

Émise par Jonathan Brossard, exerçant sous le nom commercial Probe, entrepreneur individuel, SIREN 533 060 323, 47 rue Vivienne, 75002 Paris.
À l'attention de Contoso Capital.
Objet — mission d'audit technique portant sur Acme Inc.
Date — 9 avril 2026.

1. Situation professionnelle déclarée

Je déclare exercer, parallèlement à mon activité d'audit indépendant, les fonctions de cofondateur et directeur technique d'un groupe éditant une plateforme de transfert d'argent international, dont une filiale est agréée en qualité d'établissement de paiement. Cette activité fait l'objet d'une autorisation écrite de mon employeur, dont copie peut être produite sur demande. Je porte cette situation à votre connaissance de ma propre initiative, afin que vous puissiez apprécier en pleine information mon indépendance à l'égard de la mission.

2. Déclarations relatives à la mission

Je déclare, à la date des présentes et à ma connaissance :

1. n'entretenir aucun lien capitalistique, familial, contractuel ou d'affaires, direct ou indirect, avec Acme Inc, ses dirigeants ou ses actionnaires ;
2. ne détenir aucun intérêt financier, direct ou indirect, dans Acme Inc ni dans l'issue de l'opération envisagée ;
3. n'être partie à aucun accord d'apport d'affaires, de rétrocession ou de rémunération de tiers en lien avec la mission ;
4. n'avoir exercé aucune mission antérieure, à quelque titre que ce soit, pour le compte d'Acme Inc au cours des trois dernières années ;
5. qu'Acme Inc n'exerce aucune activité concurrente de celle du groupe au sein duquel j'exerce mes fonctions salariées, sur aucun marché où celui-ci intervient ;
6. que ma rémunération au titre de la mission est forfaitaire et indépendante de mes conclusions comme de l'issue de l'opération envisagée.

3. Périmètre d'exclusion permanent

Je m'interdis d'accepter toute mission portant sur une société exerçant une activité de transfert de fonds, d'émission de monnaie électronique ou de services de paiement en concurrence directe avec le groupe au sein duquel j'exerce mes fonctions salariées.

4. Conduite de la mission

Je me suis engagé à conduire la mission avec objectivité et à formuler mes conclusions sans considération de leur incidence sur l'opération envisagée ou sur les intérêts de quiconque ; à fonder mes conclusions exclusivement sur les éléments observés et sur les entretiens menés, en distinguant dans le rapport les constats vérifiés des déclarations non vérifiées — ce que traduit la colonne « niveau d'assurance » du §2.4 et le niveau de preuve porté par chaque constat ; à n'accepter d'Acme Inc ni de ses dirigeants aucun avantage, rémunération ou libéralité ; et à n'utiliser aucune information obtenue à l'occasion de la mission à des fins étrangères à celle-ci.

5. Obligation d'information continue

Si un fait de nature à affecter mon indépendance ou à créer un conflit d'intérêts, même potentiel ou apparent, était survenu au cours de la mission, je m'étais engagé à vous en informer sans délai et par écrit, et à suspendre mes travaux jusqu'à ce que vous ayez pris position. Aucun fait de cette nature n'est survenu.