Retour au rapport de gérance 2025-2026

**Sujets connexes** Proc#174 - Revue de direction
Cartographie fonctionnelle de LoGeAs

# Audits de certification - exercice 2025-2026

| | |
|---|---|
| **Enregistrement** | Synthèse des audits de certification réalisés pendant l'exercice 2025-2026 et des actions correctives associées. Annexe au rapport de gérance (rubrique Certification). Les rapports d'audit complets, diffusables uniquement dans leur intégralité, sont conservés dans Proton. |

## Synthèse

| Marque | Type d'audit | Date | Organisme | Version auditée | NC majeures | NC mineures | Points de vigilance | Écarts levés | Décision |
|---|---|---|---|---|---|---|---|---|---|
| NF 203 (comptabilité informatisée) | Audit complet de renouvellement, à distance | 6 et 7 novembre 2025 | AFNOR Certification / INFOCERT | LoGeAs Web 11.0.2.0 | 0 | 2 | 11 | 7 | Favorable |
| NF 552 (protection des données personnelles) | Surveillance annuelle | 20 novembre 2025 | AFNOR Certification / INFOCERT | LoGeAs Web 11.0.2.00 | 0 | 4 | 21 | 1 | Favorable |

Les deux certifications sont maintenues. Aucune non-conformité majeure.

**Constats principaux :**

- Plusieurs écarts sont **maintenus d'une année sur l'autre** : il manque un suivi formel des actions correctives entre deux audits.
- Une part importante des points de vigilance NF 552 porte sur des **procédures non mises à jour** (SVN au lieu de GitLab, ProjeQtor au lieu de l'outil interne, déploiement et roadmap non formalisés, architecture technique ancienne).
- Les **tests** reviennent dans les deux audits : pas de PV de recette, pas de rapport d'exécution sur la version certifiée, documentation de test incomplète.
- Les **droits RGPD** (rectification, opposition, retrait du consentement, preuve du consentement) ne sont pas encore couverts par le logiciel.

## Écarts levés pendant les audits

| Marque | Référence | Écart d'origine | Résolution |
|---|---|---|---|
| NF 203 | AUD-I-08076 | Pas de lien entre ticket client et ticket de développement | Lien mis en place dans l'outil de ticketing |
| NF 203 | AUD-I-08077 | Pas d'enquête de satisfaction | Enquête 2024 réalisée et analysée |
| NF 203 | AUD-I-08080 | Rupture de séquence des pièces dans le FEC | Numéros de pièces externes saisis par l'utilisateur : clôturé |

| Marque | Référence | Écart d'origine | Résolution |
|---|---|---|---|
| NF 203 | AUD-I-08074 | Archive fiscale sans compte de résultat, bilan, grands livres | Documents ajoutés à l'archive fiscale |
| NF 203 | AUD-I-08068 | FEC ne précisant pas exercice clôturé ou non | Mention ajoutée dans le rapport du FEC |
| NF 203 | AUD-I-08072 | Pas de contrôle du SIREN / SIRET | Contrôle mis en place |
| NF 203 | AUD-I-08081 | Code JET 30 non implémenté | Code implémenté |
| NF 552 | 2024 n°3 | Pas de trace de l'exercice des droits | Événements RGPD tracés dans la piste d'audit |

# Écarts ouverts et actions correctives

Statuts : **NCm** non-conformité mineure, **PV** point de vigilance. « Maintenu » : écart déjà relevé l'année précédente.

## Produit - comptabilité (NF 203)

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| AUD-I-08084 NCm | Le statut « validé » d'une écriture ne s'affiche pas en consultation | Afficher le statut de l'écriture | **Traité** |
| AUD-I-08075 NCm (maintenu) | Possibilité d'ouvrir un exercice de plus de 24 mois | Correction sur la version web et mise en place d'un test | **Traité** |
| AUD-I-08079 PV (maintenu) | Balance d'ouverture laissée en brouillard | Aucune modification du logiciel. Dans LoGeAs, les saisies ne peuvent porter que sur un compte terminal. Si le compte de banque 512 utilisé en N-1 est repris tel quel dans la balance d'ouverture et que l'association ouvre ensuite un second compte bancaire, il faut créer deux sous-comptes (par exemple 512000001 pour l'ancien compte et 512000002 pour le nouveau). L'écriture de balance d'ouverture pointe alors sur un compte qui n'est plus terminal : sa structure doit être modifiée, mais pas ses montants. C'est pourquoi elle reste en brouillard. Le bilan d'ouverture reste identique au bilan de clôture de l'exercice précédent, ce qui respecte à notre sens le principe d'intangibilité. | **Justifié** : réponse à présenter à l'auditeur |

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| AUD-I-08085 PV | Pas de fonction de lettrage | Aucune modification du logiciel. LoGeAs ne gère pas de facturation au sens propre : il n'est ni certifié ni certifiable pour la facturation. Nos clients (associations, paroisses, syndicats) n'émettent pas réellement de factures : le lettrage tel que l'envisage un comptable ne nous semble donc pas primordial. Chaque écriture multi-ligne qui représente une « facture » porte néanmoins une date de paiement, qui permet de repérer les « factures » non payées. | **Justifié** : réponse à présenter à l'auditeur |
| AUD-I-08089 PV | Suppression définitive possible d'un sous-compte à solde nul | Aucune modification du logiciel à ce stade. Nous ne trouvons dans le référentiel ni exigence ni motif justifiant ce point : nous préférons le laisser en l'état et en discuter lors du prochain audit. | **À discuter** avec l'auditeur |
| AUD-I-08082 PV | Pas d'option TVA sur encaissements / débits pour les entreprises | Aucune modification du logiciel. LoGeAs est un logiciel de comptabilité, certifié NF 203 dans le seul domaine « Comptabilité » ; il n'est pas certifié pour la facturation et n'en assure pas. Le dictionnaire R12 (factures de ventes) ne nous semble donc pas applicable. | **Justifié** : réponse à présenter à l'auditeur |
| AUD-I-08073 PV (maintenu) | Code JET 240 non implémenté (tracé en 904/905) | Implémenter le code 240 | Ouvert |

## Système qualité (NF 203 et NF 552)

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| NF 552 n°8 NCm | Pas de rapport d'exécution des tests sur la version 11.0 | Produire un rapport d'exécution des tests à chaque version | **Traité** pour les versions à venir : Proc#168 interdit toute livraison sans rapport qualité validé portant sur le code exact (preuve à présenter : premier rapport validé) |
| AUD-I-08078 PV (maintenu) | Pas de PV de recette | Établir un PV de recette par version | **Traité** : recette de la beta enregistrée « Conforme » dans le rapport qualité (Proc#168) |
| AUD-I-08090 PV | Étapes de test et démarche de résolution d'erreurs non documentées | Rédiger la procédure de test | **Traité** : étapes de test, portes bloquantes et règle de décision en cas d'échec (refus, ou validation avec réserves rattachées à un ticket) dans Proc#168, mise en ligne dans Proc#169, traitement des bogues dans Proc#8 |

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| NF 552 n°9 PV | Pas de tests de performance ni de sécurité, pas de périodicité | Définir et planifier ces tests | **Traité** : tests Playwright automatisés, consultables dans la cartographie fonctionnelle – Univers Tests : test de charge (sessions simultanées, création de personnes, rapport publié sur le serveur Nono) et tests de sécurité d'accès (T57/T80/T55 comptes inconnu/désactivé/archivé, T77/T86 droits fichier, T29/T81 piste d'audit). Périodicité : exécutés à chaque run de qualification de version, rapport qualité exigé avant livraison (Proc#168) |
| NF 552 n°10 PV | Outil de bogues sans version détectée, reproductibilité, analyse des causes | Ajouter ces champs aux tickets de développement | **A discuter** : Proc#8 exige les étapes de reproduction ; champs version détectée et analyse des causes à ajouter dans l'outil |
| AUD-I-08091 PV | Tickets sans priorité ni catégorie | Ajouter priorité et catégorie aux tickets | **A Discuter** : types et niveaux de gravité définis dans Proc#8 (refonte juin 2026) ; champs à vérifier dans l'outil |
| NF 552 n°11 PV | Exploitation de la satisfaction client non formalisée | Formaliser l'analyse de l'enquête et les actions qui en découlent : procédure Proc#183 - Mesure de la satisfaction client (périodicité, questionnaire, déroulé, indicateurs et seuils d'analyse, rapport, plan d'actions suivi en revue de direction, enregistrements sur la page Questionnaires de satisfaction) | **Traité** : Proc#183 rédigée ; première enquête selon cette procédure en cours (rapport et plan d'actions à présenter à l'auditeur) |
| AUD-I-08087 / NF 552 n°7 PV | Plan produit sans lien avec les versions ; roadmap interne non formalisée | Relier le plan produit aux versions et formaliser la roadmap | **Traité** : documentation Proc#182 |
| AUD-I-08086 PV | Documentation de gestion des versions non mise à jour depuis 2018 | Mettre à jour la documentation | **A Discuter** : documentation refondue (Proc#145, janvier et août 2026) ; identification des clients par version à vérifier |

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| AUD-I-08088<br>PV | Liens vers la documentation wiki non mis à jour | Vérifier et mettre à jour les liens vers le wiki : dans la cartographie fonctionnelle (liens vers les wikis utilisateurs et vers les procédures de certification), puis sur logeas-web.fr. | **Partiel** : liens de la cartographie fonctionnelle vérifiés et mis à jour ; reste à faire : liens de logeas-web.fr |
| NF 552 n°4, 5, 6<br>PV | Procédures obsolètes : SVN au lieu de GitLab, ProjeQtor au lieu de l'outil interne ; déploiement non formalisé | Réviser les procédures selon Proc#163 | **Traité** : SVN remplacé par Git (fusion de la procédure #30 dans Proc#145, Proc#167) ; ProjeQtor remplacé par l'outil interne (Proc#8) ; déploiement formalisé (Proc#168, Proc#169, Proc#144) |
| NF 552 n°16<br>PV | Architecture technique non à jour | Mettre à jour le schéma d'architecture | **Traité** : Dossier d'Architecture Technique mis à jour (version 1.3, octobre 2026) : schéma de l'infrastructure physique refait d'après l'inventaire des machines (nœuds de virtualisation et machines virtuelles du datacenter de Saint-Gaudens, liaisons fibre et LTE, NAS de sauvegarde des locaux de Labarthe-Inard), zones des locaux et liste des sites hébergés corrigées. Complété par la cartographie des flux de données personnelles |

## Protection des données (NF 552)

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| NF 552 n°2 NCm (maintenu) | Sauvegardes faites par l'utilisateur depuis le logiciel (fichiers SQL) non chiffrées, effacées du serveur après 8 jours. Les sauvegardes du plan de sauvegarde (Proc#130) ne sont pas concernées : les bases chiffrées y sont copiées telles quelles | Aucune modification du logiciel à ce stade, comme déjà évoqué lors des audits précédents. Ces sauvegardes sont faites par nos utilisateurs eux-mêmes, en grande majorité des bénévoles peu familiers de l'informatique. Les chiffrer imposerait de conserver une clé ou un mot de passe en dehors du logiciel : en cas de perte, la sauvegarde deviendrait irrécupérable. Le risque d'avoir des sauvegardes impossibles à restaurer, au moment même où l'on en a besoin, nous paraît plus grave que celui de leur divulgation. Les sauvegardes du plan de sauvegarde, elles, restent chiffrées. | **À discuter** avec l'auditeur |

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| NF 552 n°18 NCm | Cartographies non restituées dans un format exploitable (JSON, XML, CSV) | Ajouter un export de la cartographie : MCD (modèle conceptuel de données) interactif, généré directement à partir des classes Angular du logiciel, donc toujours aligné sur le code de la version livrée. Les entités, attributs et relations sont déclarés dans le code ; chaque attribut porte sa qualification (nominatif, obligatoire, sensible). Le diagramme se filtre et se réorganise à l'écran, et ce qui est affiché s'exporte en **SVG** (diagramme), **CSV** (dictionnaire des attributs et liste des relations) et **JSON** (modèle complet). Chaque export JSON commence par des informations de traçabilité (application, version, base, périmètre) et chaque export est accompagné d'un texte explicatif sur son contenu et la provenance de la qualification des données. | **Traité** : disponible dans LoGeAs Web (menu **États > Microscope**), pour le modèle de la base du client, et dans la cartographie fonctionnelle (**MCDs des bases de données**), pour l'ensemble des bases |
| NF 552 n°19 NCm | Pas de preuve du consentement de la personne concernée | Recueil du consentement dans LoGeAs Web (Administration > Consentement RGPD) : modèle versionné et validé avant envoi, lien personnel vers un formulaire public ou formulaire papier, une finalité par utilisation. Chaque réponse est conservée sans modification possible avec le texte figé présenté à la personne, la version et l'empreinte du modèle, les choix, la date, et en ligne l'adresse IP et le navigateur ; le formulaire rempli est réaffichable tel que la personne l'a vu. | **En cours** : développé, livré avec la prochaine version (couverture NF 552, documentation utilisateur) |
| NF 552 n°22 PV | Pas de fonction de retrait du consentement | La personne retire son consentement en répondant à nouveau, par un nouveau lien ou sur papier : la réponse la plus récente fait foi. | **En cours** : développé, livré avec la prochaine version (couverture NF 552) |
| NF 552 n°20, 21 PV | Pas de fonction de rectification (utilisateur standard), d'opposition | Ajouter ces fonctions | Ouvert |

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| NF 552 n°1 PV (maintenu) | Pas de contrôle des champs texte libre | Aucune modification du logiciel à ce stade, comme déjà évoqué lors des audits précédents. Nos utilisateurs, en grande majorité des bénévoles peu familiers de l'informatique, se servent des champs texte libre pour noter des informations utiles à la vie de l'association. Un contrôle par liste de mots serait peu fiable : il bloquerait des saisies légitimes et laisserait passer des formulations non prévues. Il risquerait surtout de pousser les utilisateurs à noter ces informations hors du logiciel, là où elles ne sont plus protégées. Nous avons fait le choix inverse : toutes les données sont déclarées sensibles au sens de l'article 9 du RGPD et protégées comme telles (voir NF 552 n°14, 15). | **À discuter** avec l'auditeur |
| NF 552 n°3 PV (maintenu) | Pas de documentation d'administration sur les obligations de traitement des données | Rédiger un guide RGPD de l'administrateur dans le wiki utilisateur : rôles responsable de traitement / sous-traitant, minimisation et champs texte libre, consentement, réponse aux demandes de droits (accès, portabilité, oubli, rectification, opposition), conservation, droits d'accès, protection des sauvegardes, registre des traitements, violation de données. | **Traité** : RGPD : guide de l'administrateur |
| NF 552 n°14, 15 PV | Pas de document déclarant toutes les données comme sensibles (art. 9 RGPD) ; cartographie des flux et MCD à présenter | Compléter la documentation RGPD | **Traité** : le document technique Protection des données dans le développement déclare toutes les données comme sensibles (article 9) ; le MCD est disponible dans le logiciel et la cartographie fonctionnelle (voir NF 552 n°18) ; la cartographie des flux de données personnelles décrit les entrées, lieux de stockage, services externes, envois et sous-traitants |

| Référence | Constat | Action corrective proposée | État |
|---|---|---|---|
| NF 552 n°17 PV | Pas d'archivage des versions de la cartographie | Aucune modification à ce stade. La cartographie fonctionnelle est une base de données alimentée chaque jour par les évolutions et les changements : nous n'avons pas aujourd'hui de moyen de la figer, si ce n'est les sauvegardes quotidiennes de cette base, qui peuvent être restaurées en cas de contrôle. Les solutions envisageables seront discutées lors du prochain audit. | **À discuter** avec l'auditeur |
| NF 552 n°13 PV | Champ « nominatif » mal affiché dans la cartographie | Corriger l'affichage | Ouvert |
| NF 552 n°12 PV | Pas de procédure de notification des failles de sécurité aux clients | Créer la procédure Proc#181 - Faille de sécurité et violation de données : information des clients : signalement, confinement, qualification, information des clients au plus tard 48 heures après la prise de connaissance pour leur permettre de notifier la CNIL dans les 72 heures, registre des violations. | **Traité** : Proc#181 créée et validée |
| NF 552 n°23 PV | Bogue à l'export de la piste d'audit | Corriger l'export | Ouvert |
| NF 552 n°24 PV | Minimisation des données (privacy by design) non documentée | Formaliser la protection des données dès la conception : règle « Protection des données » ajoutée à Proc#179 et document technique Protection des données dans le développement (minimisation, déclaration des données nominatives, droits des personnes, conservation, journaux, données de test, sécurité). | **En cours** : modification de Proc#179 à valider et approuver |
| NF 552 n°25 PV | Vulnérabilités (audits STOIK) non classées selon un référentiel reconnu (OWASP) | Aucune modification. Interrogé, Stoïk indique que l'OWASP Top 10 ne couvre que les vulnérabilités des applications web, alors que ses scans portent sur l'ensemble de l'infrastructure exposée, y compris les identifiants compromis : ce référentiel ne peut donc pas s'appliquer à ses résultats. En revanche, chaque vulnérabilité relevée est rattachée à sa référence **CVE** quand elle en a une, le référentiel international des vulnérabilités connues. Méthodologie : scan externe Stoïk. | **Justifié** : réponse à présenter à l'auditeur |

# Bilan au 16 octobre 2026

La remise à plat des procédures de l'été 2026 traite les écarts portant sur les procédures obsolètes et sur les tests : les PV de recette et rapports d'exécution sont désormais produits par la chaîne de

qualification et de livraison (Proc#168), dont la première application devra être présentée aux auditeurs. Les tests de performance et de sécurité sont automatisés et exécutés à chaque version (NF 552 n°9). La notification des failles de sécurité aux clients fait l'objet d'une nouvelle procédure, Proc#181.
Le Dossier d'Architecture Technique et son schéma d'infrastructure sont à jour (NF 552 n°16), et une cartographie des flux de données personnelles a été établie (NF 552 n°14, 15).
La cartographie des données est restituée dans des formats exploitables : un MCD interactif, généré à partir du code et exportable en SVG, CSV et JSON, est disponible dans le logiciel et dans la cartographie fonctionnelle (NF 552 n°18).
Un guide RGPD de l'administrateur informe nos clients de leurs obligations et des outils du logiciel pour les remplir (NF 552 n°3).
L'exploitation de la satisfaction client est formalisée par la procédure Proc#183, dont la première enquête est en cours (NF 552 n°11).
Quatre écarts sont justifiés sans modification du logiciel (AUD-I-08079, AUD-I-08085, AUD-I-08082, NF 552 n°25) et quatre sont à discuter avec l'auditeur (AUD-I-08089, NF 552 n°1, NF 552 n°2, NF 552 n°17) : ces réponses seront présentées lors du prochain audit.
Le recueil, la preuve et le retrait du consentement sont couverts par un nouvel outil de LoGeAs Web, livré avec la prochaine version : lien personnel vers un formulaire public ou formulaire papier, preuve conservée avec le texte exact présenté à la personne (NF 552 n°19 et n°22).
Restent ouverts : les autres écarts produit (comptabilité et protection des données), ainsi que le plan produit et la roadmap.

## Prochains audits

*[À COMPLÉTER : dates prévues des audits NF 203 et NF 552 de l'automne 2026.]*

From:
https://wiki-logeas.fr/certif/ - **dokuwiki-certif**

Permanent link:
**https://wiki-logeas.fr/certif/doku.php?id=certif:revuedirection:2025-2026:audits&rev=1792394569**

Last update: **2026/10/19 09:22**