SaaS**Control**

RAPPORT D'AUDIT — 2026

SaaS & AI Risk Assessment

Diagnostic des applications SaaS, usages IA et risques de conformité

SaaSControl Demo

Généré le 16/06/2026 à 12:38

2	2	2	2	79
APPLICATIONS	AVEC IA	NON APPROUVÉES	ÉLEVÉ / CRITIQUE	SCORE MOYEN

Résumé exécutif

2	2	2	2	79
TOTAL APPLICATIONS	APPLICATIONS AVEC IA	NON APPROUVÉES OU INCONNUES	RISQUE ÉLEVÉ / CRITIQUE	SCORE MOYEN

Ce registre comporte 2 application(s) classée(s) Élevé ou Critique. Une revue de gouvernance prioritaire est recommandée.

1 application(s) n'ont pas de date de révision enregistrée. Définir un calendrier de révision est fortement conseillé.

2 application(s) font usage de l'IA. Ces usages doivent être documentés et encadrés par une politique interne.

2 application(s) ne sont pas encore approuvées ou ont un statut inconnu. Leur usage doit être clarifié avant toute extension.

Méthodologie

- Inventaire des applications SaaS et IA utilisées par l'organisation.
- Qualification des données traitées par chaque application : données personnelles, sensibles, financières, de santé, code source, données clients.
- Évaluation de la criticité métier et de l'impact opérationnel attendu.
- Prise en compte du statut d'approbation pour identifier les outils inconnus, rejetés ou en cours de révision.
- Détection des usages IA et du type d'IA pour appuyer la gouvernance IA et les politiques internes.
- Calcul d'un score de risque de 0 à 100, traduit en niveau Faible, Moyen, Élevé ou Critique.
- Production de recommandations prioritaires pour planifier la gouvernance et les preuves d'audit.

Top risques

Applications classées par score de risque décroissant (10 premières).

APPLICATION	SCORE	NIVEAU	CRITICITÉ	STATUT	FACTEURS DE RISQUE
ChatGPT OpenAI	**80**	**Critique**	Élevé	En revue	Utilise des capacités IA et peut nécessiter une revue AI Act et gouvernance des données.; Traite des données personnelles et doit figurer au registre RGPD avec revue DPA.; Traite des données clients et doit être examiné au regard des obligations de confidentialité.; Criticité métier Élevé : renforce les exigences de continuité et de sécurité.; Statut d'approbation En revue : l'usage doit être contrôlé ou revu.; Aucune date de révision n'est enregistrée.
Claude Anthropic	**78**	**Critique**	Élevé	En revue	Utilise des capacités IA et peut nécessiter une revue AI Act et gouvernance des données.; L'IA générative accroît les exigences de confidentialité, de qualité des sorties et de revue fournisseur.; Traite des données personnelles et doit figurer au registre RGPD avec revue DPA.; Traite des données clients et doit être examiné au regard des obligations de confidentialité.; Criticité métier Élevé : renforce les exigences de continuité et de sécurité.; Statut d'approbation En revue : l'usage doit être contrôlé ou revu.

Cartographie SaaS / IA

Inventaire complet des applications enregistrées, classées par score de risque décroissant.

APPLICATION	ÉDITEUR	CATÉGORIE	IA	DONNÉES TRAITÉES	CRITICITÉ	STATUT	SCORE	NIVEAU
ChatGPT	OpenAI	AI	Oui	Données personnelles, Données clients	Élevé	En revue	**80**	**Critique**
Claude	Anthropic	AI	Oui	Données personnelles, Données clients	Élevé	En revue	**78**	**Critique**

Focus IA — Gouvernance des usages IA

2 application(s) identifiée(s) avec usage IA. Ces applications appellent une attention particulière au regard du RGPD et de l'AI Act.

APPLICATION	TYPE D'IA	SCORE	NIVEAU	DONNÉES TRAITÉES	POINTS D'ATTENTION
ChatGPT OpenAI	Non renseigné	**80**	**Critique**	Données personnelles, Données clients	Documenter le cas d'usage, vérifier les contrôles fournisseur, clarifier les traitements de données personnelles et définir les règles d'usage collaborateur.
Claude Anthropic	IA générative	**78**	**Critique**	Données personnelles, Données clients	Documenter le cas d'usage, vérifier les contrôles fournisseur, clarifier les traitements de données personnelles et définir les règles d'usage collaborateur.

Cadre réglementaire applicable : Les outils d'IA générative, prédictive ou automatisée peuvent être soumis au RGPD (traitement de données personnelles), à l'AI Act européen (systèmes à risque) et aux politiques internes de gouvernance des données. Une revue juridique est recommandée pour les usages à fort impact.

Recommandations prioritaires

- Revoir en priorité les applications Critique et Élevé non approuvées.
- Attribuer un responsable métier à chaque application du registre.
- Mettre à jour les dates de révision et définir un calendrier de révision récurrent.
- Documenter les cas d'usage IA, les données en entrée et les mesures de contrôle attendues.
- Vérifier les traitements de données personnelles, les contrats fournisseurs et les règles de rétention.
- Formaliser une politique d'usage IA pour les collaborateurs et les prestataires.
- Préparer les preuves d'audit pour la revue fournisseur, le contrôle des accès et la réponse à incident.

Prochaines actions recommandées

Actions concrètes à engager à l'issue de la lecture de ce rapport.

Lancer une revue de gouvernance ciblée sur les applications Élevé et Critique identifiées dans ce rapport.

Statuer sur chaque application non approuvée ou inconnue : approbation formelle, mise en observation ou désactivation.

Rédiger ou mettre à jour la politique d'usage IA interne en couvrant les outils identifiés dans ce rapport.

Planifier une révision des applications sans date de révision enregistrée et établir un calendrier formel.

Vérifier la présence de contrats de sous-traitance (DPA) pour chaque éditeur traitant des données personnelles.

Préparer un dossier de preuves d'audit (accès, contrats, politiques) pour les prochaines obligations réglementaires RGPD, NIS2 ou AI Act.

Légende de scoring

- Faible (0–24) : facteurs de risque limités, surveillance standard.
- Moyen (25–49) : révision recommandée, surveillance renforcée.
- Élevé (50–74) : remédiation prioritaire attendue.
- Critique (75–100) : revue de gouvernance immédiate requise.

Note de prudence : *Ce rapport constitue un diagnostic indicatif basé sur les informations transmises. Il ne remplace pas un audit juridique, sécurité ou conformité complet. Les scores et niveaux de risque sont des indicateurs de priorisation et non des certifications de conformité. SaaSControl recommande de compléter cette analyse par une revue juridique et technique appropriée.*