Checklist gouvernance du shadow IA

20 points de contrôle pour passer de l'usage subi à l'usage piloté. À dérouler dans l'ordre : **voir**, puis **cadrer**, puis **sécuriser**, puis **outiller**, puis **mesurer**. Interdire avant d'avoir vu ne fait que déplacer l'usage vers le téléphone personnel.

> **60 %** des organisations n'ont pas confiance dans leur capacité à identifier l'usage d'outils IA non approuvés dans leur environnement, et **60 %** n'ont aucune visibilité sur les prompts envoyés par leurs collaborateurs. — Cisco Cybersecurity Readiness Index 2025

1 Voir — cartographier ce qui tourne déjà

- [ ] **Inventorier les outils IA réellement utilisés** — journaux proxy/DNS, extensions de navigateur installées, notes de frais et abonnements SaaS payés hors DSI.
- [ ] **Identifier les assistants IA déjà embarqués** dans les SaaS que vous avez signés (CRM, suite bureautique, ITSM, outils RH) et qui sont activés par défaut.
- [ ] **Qualifier les usages par service** — qui utilise quoi, sur quel type de contenu, à quelle fréquence. Agrégé par équipe, jamais nominatif.
- [ ] **Repérer les usages à risque élevé** — données clients, contrats, code source, données RH ou financières collés dans un outil grand public.

2 Cadrer — une politique applicable, pas une interdiction

- [ ] **Classer vos données par niveau de sensibilité** et statuer explicitement, pour chaque niveau, ce qui peut être soumis à une IA et dans quel outil.
- [ ] **Publier une liste d'outils autorisés** — et surtout une procédure simple pour en faire ajouter un. Sans porte d'entrée, le contournement est garanti.
- [ ] **Définir les cas nécessitant une validation humaine** — toute action qui écrit dans un système de production, engage l'entreprise ou touche un client.
- [ ] **Rattacher la politique à vos obligations** — AI Act (classification par niveau de risque, transparence, AI literacy), RGPD, secret des affaires, engagements clients.

3 Sécuriser — données, contrats, traçabilité

- [ ] **Vérifier les clauses de non-réentraînement** sur vos données pour chaque fournisseur retenu, en version écrite et contractuelle — pas dans une FAQ marketing.
- [ ] **Documenter l'hébergement et les sous-traitants** — localisation des traitements, DPA signé, registre des sous-traitants à jour.
- [ ] **Journaliser les usages sensibles** — qui a soumis quel type de donnée à quel outil, avec une durée de conservation définie.
- [ ] **Gérer le cycle de vie des accès** — SSO obligatoire, révocation testée au départ d'un collaborateur, aucun compte personnel sur un usage professionnel.

4 Outiller — l'alternative doit être plus pratique que le contournement

- [ ] **Déployer un outil validé au moins aussi bon** que celui que vos équipes utilisent en douce. Un outil interne moins performant ne sera pas adopté, il sera contourné.
- [ ] **Mettre à disposition une bibliothèque de prompts validés** par métier, pour que les équipes partent de modèles éprouvés au lieu d'improviser chacune dans son coin.
- [ ] **Encapsuler les cas récurrents dans des mini-apps** — le prompt, les données autorisées et les garde-fous sont figés une fois pour toutes, pas rejoués à chaque usage.
- [ ] **Former sur les cas d'usage réels du poste** — une sensibilisation générique ne change pas les comportements ; un cas d'usage qui fait gagner du temps, si.

5 Mesurer — ce qui n'est pas mesuré n'est pas piloté

- [ ] **Suivre le taux d'adoption par service** — licences actives vs licences payées, et écart entre services. C'est votre premier arbitrage budgétaire.
- [ ] **Suivre la part d'usages hors cadre** dans le temps. C'est l'indicateur qui dit si votre politique fonctionne ou si elle est simplement ignorée.
- [ ] **Distinguer usage et valeur** — ouvrir l'outil tous les jours pour reformuler des e-mails ne vaut pas un processus automatisé. Mesurez les deux.
- [ ] **Rapporter au comité de direction trimestriellement** — coût par outil, adoption par service, incidents évités, écarts de conformité traités.

✓ Les trois erreurs qui coûtent le plus cher

- [ ] **Bloquer avant de voir.** L'interdiction déplace l'usage vers le téléphone personnel, où vous n'avez plus aucune visibilité ni recours.
- [ ] **Surveiller le contenu individuel.** Vous perdez la confiance des équipes, et avec elle toute remontée volontaire d'usage. Mesurez des flux, pas des personnes.
- [ ] **Déployer sans mesurer.** Six mois plus tard, le comité de direction demande « ça sert à quoi ? » et la DSI n'a aucun chiffre à présenter.