
CHECKLIST
IA & CYBER PRÉPARATION
EN 10 POINTS
AGILENS

🚨 Checklist IA & Cyber Préparation 🔐 2026 (en 10 points)

Réduire le risque IA (GenAI, copilots, agents) sans ralentir l'innovation

À qui s'adresse ce document ?
DG/DAF/DRH, DSI, RSSI, responsables Data/IA, responsables Risques/Conformité.

Objectif
Évaluer en moins de 30 minutes votre niveau de préparation **IA & Cyber** et identifier les **10 actions prioritaires** pour réduire :

- Fuite de données via GenAI / copilots / connecteurs,
- Erreurs de configuration et droits excessifs,
- Fraude (deepfake, usurpation, faux RIB, social engineering assisté par IA),
- Risques fournisseurs liés aux outils IA.

Mode d'emploi

- Pour chaque point, cochez votre niveau : **0 / 1 / 2**
- Additionnez le score (max **20**)
- Utilisez la page "Plan 10 jours" en fin de document pour prioriser.

Grille de score (simple)

- **0 = Non en place / ad hoc** (dépend des individus, pas de preuve)
- **1 = Partiel** (en place sur un périmètre limité, preuves incomplètes)
- **2 = Maîtrisé** (processus + preuves + contrôle périodique)

Interprétation

- **0–7 : Exposition élevée** → risque de fuite/incident/fraude sous 6 mois
- **8–14 : Niveau intermédiaire** → prioriser 3–4 chantiers structurants
- **15–20 : Bon niveau** → focus amélioration continue, auditabilité, agents IA

Les 10 points de la checklist (avec preuves attendues)

1) Inventaire des usages IA (y compris “Shadow AI”)
Objectif : savoir *qui* utilise *quoi*, *sur quelles données*, *avec quels connecteurs*.
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Liste officielle des outils IA autorisés ?
- Détection des usages non autorisés (proxy, CASB, logs, dépenses, extensions navigateur) ?

  Preuves attendues
- Registre des outils IA (SaaS, plugins, copilots, APIs), owners, finalité, données, risques, statut “autorisé/interdit”.

2) Classification des données + règles “ce qui peut aller dans l’IA”
Objectif : éviter la fuite de données sensibles (client, RH, finance, IP, secrets).
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Existe-t-il une règle claire : *données interdites / autorisées / autorisées sous conditions* ?
- Les équipes savent-elles reconnaître une donnée sensible ?

  Preuves attendues
- Matrice de classification (Public/Interne/Confidentiel/Sensible), exemples concrets, procédure d’exception.

3) Gouvernance GenAI : politique d’usage + processus d’exception
Objectif : “libérer” les usages à valeur tout en cadrant risques.
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Politique d’usage GenAI signée et comprise ?
- Circuit d’exception (cas d’usage, validation, durée, contrôles) ?

  Preuves attendues
- Politique 1–2 pages + formulaire d’exception + registre des exceptions + revue trimestrielle.

4) Sécurisation des identités (le vrai périmètre IA)
Objectif : réduire l'impact d'une compromission (compte, session, token, API key).
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- MFA partout (messagerie, SaaS, admin, VPN, accès cloud) ?
- Revue des droits et suppression des comptes dormants ?
- Comptes à privilèges isolés (PAM) ?
  Preuves attendues
- Taux MFA, rapports de revue d'accès, inventaire comptes admin, politique API keys, rotation.

5) Contrôles techniques "anti-fuite" sur canaux IA
Objectif : empêcher/corriger l'exfiltration (copier-coller, upload, connecteurs).
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- DLP (mail, web, endpoint, cloud) ?
- Blocage/alerte sur uploads sensibles vers IA publiques ?
- Journalisation des accès aux outils IA ?
  Preuves attendues
- Règles DLP, alertes, logs, playbook de traitement, mesures de durcissement.

6) Sécurité des outils IA "internes" (RAG, agents, API, plugins)
Objectif : sécuriser ce que vous construisez (et pas seulement ce que vous achetez).
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Revue sécurité avant mise en prod (threat model, pentest, secrets scanning) ?
- Séparation environnements (dev/test/prod) et secrets vault ?
- Contrôle des connecteurs (SharePoint, Drive, CRM, Jira) ?
  Preuves attendues
- Dossier d'architecture, threat model, registre des secrets, règles de connecteurs, tests sécurité.

7) Risque "fournisseurs IA" (due diligence + clauses)
Objectif : maîtriser où part la donnée + ce que fait le fournisseur avec.
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Questionnaire sécurité standardisé pour outils IA ?
- Clauses contractuelles (données, conservation, sous-traitants, entraînement, localisation) ?
  Preuves attendues
- Fiche d'évaluation fournisseur, exigences minimales, validation RSSI/Legal, inventaire des sous-traitants critiques.

8) Prévention de la fraude assistée par IA (deepfake, usurpation, faux ordres)
Objectif : réduire les pertes financières et la manipulation humaine.
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Procédure “2 canaux” (vérification hors bande) pour virements / changements RIB / demandes urgentes ?
- Mot de passe/phrase de validation pour demandes sensibles ?
- Sensibilisation ciblée Finance/RH/Assistantes/Comex ?
  Preuves attendues
- Procédure anti-fraude, scripts de vérification, journal des validations, formation dédiée, tests (phishing vishing).

9) Détection & réponse : logs, monitoring, playbooks IA
Objectif : voir les signaux faibles (accès anormaux, connecteurs, exfiltration).
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Logs centralisés (SIEM) sur identité + messagerie + cloud + outils IA ?
- Playbooks : fuite via GenAI, token compromis, connecteur exposé ?
  Preuves attendues
- Catalogue de logs, règles de détection, procédures d’escalade, exercices de crise (tabletop).

10) Culture & “qualité” : usage sûr + validation des sorties IA
Objectif : réduire erreurs, hallucinations, divulgations accidentelles, conformité.
0 / 1 / 2 ☐ / ☐ / ☐
Tests rapides

- Formation courte et répétée (10–15 min) + mémo “prompt & data rules” ?
- Règle “humain responsable” + validation avant décision (juridique, RH, finance, médical, etc.) ?
  Preuves attendues
- Micro-learning, charte d’usage, checklist de validation, processus d’approbation pour contenus sensibles.

Synthèse (1 page) — Score + priorités

⇨ Votre score total : ____ / 20

Top 3 risques probables si score < 10

1. Fuite de données via outils IA non maîtrisés + connecteurs
2. Compromission d'identité (MFA/privileges insuffisants)
3. Fraude (virement / changement RIB / usurpation de dirigeant)

Vos 3 priorités 10 jours

- Priorité 1 : _____
- Priorité 2 : _____
- Priorité 3 : _____

Plan d'action "10 jours" (prêt à exécuter)

J1–J2 : cadrage & inventaire

- Lister outils IA utilisés + owners + données (même approximatif)
- Acter outils autorisés/interdits provisoires

J3–J5 : garde-fous immédiats

- Règle "données interdites" + politique courte
- MFA/accès : corriger comptes à risque + admins + comptes dormants
- Lancer procédure anti-fraude "2 canaux" sur paiements et RIB

J6–J8 : contrôles & preuves

- DLP/alerting minimum sur canaux critiques
- Centraliser logs identité + mail + cloud + outils IA

J9–J10 : formaliser & embarquer

- Processus d'exception + registre
- Mini formation (15 min) + mémo de 1 page
- Revue "fournisseurs IA" des outils en place

Annexes

Annexe A — Politique d'usage GenAI (structure en 10 lignes)

1. Outils autorisés / interdits
2. Données interdites (PII, finance, RH, secrets, client…)
3. Règles d'upload de documents + connecteurs
4. Interdiction de coller des identifiants / secrets / API keys
5. Règles de partage de résultats (internes / externes)
6. Règles de relecture humaine / responsabilité
7. Exceptions (qui valide, combien de temps, quelles preuves)
8. Journalisation / auditabilité
9. Signalement incident
10. Sanctions / rappels + contact sécurité

Annexe B — Due diligence "outil IA" (10 questions)

- Données utilisées pour entraîner des modèles : oui/non ? opt-out ?
- Où sont stockées les données ? durée de rétention ?
- Chiffrement au repos/en transit ?
- Auth (SSO/SAML), MFA, RBAC, logs admin ?
- Sous-traitants et localisation ?
- Export des logs possible ?
- Processus de vulnérabilités / pentest / bug bounty ?
- Ségrégation tenante ?
- Clauses incident : délais de notification ?
- DPA / conformité (selon votre contexte) ?