Grille 3 — Sécurité, audit et contrôle interne

ADVISORE · Webinaire du 8 décembre 2026 · livrable de l'exposé 3

> Objectif : disposer d'une liste de contrôles qu'un auditeur exigera, avec la preuve à produire pour chacun. 28 contrôles, 6 familles.

Comment l'utiliser

Pour chaque ligne : notez **Constaté** (O = en place, P = partiel, N = absent) et l'**écart** en une phrase. Un contrôle sans preuve écrite vaut **N** : l'auditeur ne juge pas l'intention, il juge le dossier.

Statut	Signification
O	Contrôle en place et prouvable immédiatement
P	En place mais non documenté, ou partiel
N	Absent, ou aucune preuve disponible

A. Identité, accès, autorisations (5)

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
A1	Comptes nominatifs	Aucun compte partagé pour l'agent ou ses opérateurs	Liste des comptes, propriétaire, date de création		
A2	Principe du moindre privilège	L'agent n'a que les droits nécessaires à sa tâche	Matrice des droits par rôle, validée		
A3	Authentification forte	MFA sur les comptes d'administration et les accès au modèle	Capture de la politique MFA, taux d'application		
A4	Révocation	Un départ ou un incident se traduit par un retrait d'accès en moins d'une heure	Procédure écrite + journal des révocations		
A5	Comptes techniques	Clés et jetons identifiés, stockés hors du code, rotation planifiée	Inventaire des secrets, date de dernière rotation		

B. Données et cloisonnement (6)

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
B1	Cartographie des données	On sait quelles données l'agent lit, écrit et conserve	Registre des traitements à jour		
B2	Base légale	Chaque traitement a une base légale documentée	Fiche de traitement, mention d'information		

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
B3	Minimisation	L'agent ne reçoit que les champs utiles, pas des extractions entières	Schéma des flux, exemple de requête		
B4	Cloisonnement	Les données d'un client ou d'une entité ne peuvent pas fuiter vers une autre	Test de cloisonnement daté, résultat		
B5	Localisation	Le lieu de traitement et de stockage est connu et accepté par le client	Contrat, annexe de localisation		
B6	Conservation et effacement	Durées définies, effacement effectif et vérifiable	Politique de rétention + preuve de purge		

C. Traçabilité et journalisation (5)

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
C1	Journal des appels	Chaque appel au modèle est journalisé : horodatage, utilisateur, cas d'usage, coût	Extrait de journal, rétention		
C2	Journal des actions	Chaque écriture de l'agent dans un système métier est tracée	Extrait de piste d'audit applicative		
C3	Corrélation	Une action peut être reliée à une demande, un utilisateur et une décision	Exemple de reconstitution de bout en bout		
C4	Intégrité des journaux	Les journaux ne peuvent pas être modifiés ou supprimés par l'exploitant	Configuration WORM / copie externe		
C5	Conservation des traces	Durée alignée sur les obligations (souvent 12 à 60 mois selon le secteur)	Politique + preuve de rétention		

D. Supervision humaine et garde-fous (4)

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
D1	Validation avant impact	Toute action à effet externe (paiement, envoi client, écriture comptable) passe par une validation	Schéma du circuit, capture de l'écran de validation		
D2	Limites dures	Plafonds de dépense, de volume et de portée configurés et testés	Configuration + test de dépassement		
D3	Gestion des erreurs	Comportement en cas d'échec défini : arrêt, repli, alerte — jamais de poursuite silencieuse	Procédure + extrait de test d'échec		
D4	Recours	Un utilisateur peut contester une décision et obtenir une correction	Canal de recours documenté		

E. Cycle de vie, modèles et fournisseurs (5)

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
E1	Inventaire des modèles	Version, fournisseur, date de déploiement de chaque modèle utilisé	Registre des modèles		
E2	Changement de version	Une mise à jour du fournisseur déclenche une revue et des tests	Procédure + journal des changements		
E3	Évaluation	Qualité mesurée sur un jeu de cas de référence, avant et après changement	Rapport d'évaluation daté		
E4	Fournisseur	Engagements contractuels : sous-traitance, localisation, notification d'incident, réversibilité	Contrat, annexes		
E5	Fin de vie	Procédure de retrait : données reprises, accès coupés, preuve de suppression	Plan de sortie testé		

F. Audit et preuves (3)

#	Contrôle	Exigence	Preuve attendue	Constaté	Écart
F1	Dossier d'audit	Les preuves A à E sont rassemblées, datées, accessibles en un endroit	Index du dossier, dernière revue		
F2	Revue périodique	Revue des accès et des journaux au moins trimestrielle	Compte rendu de revue signé		
F3	Test d'incident	Un incident a été simulé : détection, arrêt, communication, retour d'expérience	Rapport de simulation		

Synthèse

Famille	Contrôles	O	P	N
A. Identité et accès	5			
B. Données et cloisonnement	6			
C. Traçabilité	5			
D. Supervision	4			
E. Cycle de vie	5			
F. Audit et preuves	3			
Total	**28**			

Règle de lecture : un seul **N** sur les familles B, C ou D interdit la mise en production sur des données réelles. Un **N** sur A ou E impose un plan de remédiation daté avant la fin du pilote.

Les trois questions que l'auditeur posera en premier

1. **« Montrez-moi une action de l'agent, son journal et la validation qui l'a précédée. »**
2. **« Si le fournisseur disparaît demain, que devient le service, et en combien de temps ? »**

3. **« Qui a relu les accès le trimestre dernier, et qu'a-t-il changé ? »**

Si l'une des trois réponses est « on va le faire », le contrôle est à **N**.
