



EXEMPLE FIL ROUGE

Un mois après le déploiement de « Margaux » et l'incident #4, Lendari mesure la maturité de sa gouvernance agentique. Audit conduit par Camille Roussel (DDAO).

1 Informations Générales

ORGANISATION

Lendari - e-commerce mode (120 M€, 90 salariés)

RESPONSABLE DE L'AUDIT

Camille Roussel (DDAO)

DATE DE L'AUDIT

10/06/2026

PÉRIMÈTRE ÉVALUÉ

Agent « Margaux » (SAV & retours niv.1) + cadre de gouvernance Lendari

OBJECTIF DE L'AUDIT

Mesurer la maturité post-incident #4 et cadrer 30 jours d'actions prioritaires

2 Grille d'Audit - Maturité sur 8 Domaines

DOMAINE ÉVALUÉ	CRITÈRES CLÉS	MATURITÉ (1 À 5)	PREUVE / COMMENTAIRE
Gouvernance	Cadre défini · rôles clairs	1 2 3 4 5	Constitution v1.0 · DDAO · comité
Stratégie & alignement	Alignement · objectifs par usage	1 2 3 4 5	Mandat ACF-13 · KPI (ACF-06)
Données	Qualité · classification · RGPD	1 2 3 4 5	Incident #4 : désync · pas de classif.
Technologie	Architecture · outils · résilience	1 2 3 4 5	Kill switch ACF-07 · dépend. LLM
Sécurité & conformité	Sécurité · AI Act · gestion des risques	1 2 3 4 5	DPO · RGPD à jour · DPIA en cours
Supervision & contrôle	Surveillance · alertes · kill switch	1 2 3 4 5	Registre ACF-09 · revue hebdo · alerte
Compétences & culture	Compétences · formation · culture	1 2 3 4 5	Savoir sur 2 pers. · pas de formation
Performance & valeur	Indicateurs · valeur · amélioration	1 2 3 4 5	CSAT 4,2 · -30 % tickets · ROI à venir

1 Initial - ad hoc 2 Réactif - peu formalisé 3 Défini - documenté 4 Maîtrisé - mesuré & contrôlé
5 Optimal - optimisé & innovant

Niveau de maturité global (moyenne des 8 domaines) : 2,9 / 5 RÉACTIF



EXEMPLE FIL ROUGE

Lendari lit son score (2,9 / 5 - Réactif), identifie ses forces et ses écarts majeurs, puis priorise les actions.

3 INTERPRÉTATION DU SCORE

SCORE MOYEN	NIVEAU	INTERPRÉTATION	ACTIONS RECOMMANDÉES
1,0 – 1,9	INITIAL	Gouvernance inexistante ou très faible. Risques élevés, maîtrise insuffisante.	Poser les fondations : cadre, rôles, politiques de base, sensibilisation.
2,0 – 2,9	RÉACTIF	Démarche en cours mais non structurée. Vulnérabilités importantes.	Formaliser les processus clés, documenter et renforcer les contrôles.
3,0 – 3,9	DÉFINI	Gouvernance en place mais perfectible. Cohérence à améliorer.	Renforcer la mesure, la supervision et l'alignement stratégique.
4,0 – 4,4	MAÎTRISÉ	Gouvernance robuste et mesurée. Bonne maîtrise des risques.	Optimiser l'efficacité et la valeur. Automatiser certains contrôles.
4,5 – 5,0	OPTIMAL	Gouvernance de référence. Culture d'amélioration continue.	Innover, partager les bonnes pratiques, viser l'excellence.

4 ANALYSE DES RÉSULTATS

✓ FORCES IDENTIFIÉES

- ✓ Supervision & contrôle mature (4/5) : kill switch + registre + revue
- ✓ Cadre de gouvernance posé : Constitution agentique + DDAO
- ✓ Réflexe incident éprouvé - incident #4 maîtrisé en 40 min

⚠ FAIBLESSES / ÉCARTS MAJEURS

- ! Gouvernance des données immature (2/5) - cause racine de l'incident #4
- ! Compétences concentrées sur 2 personnes : risque de continuité
- ! Conformité AI Act à formaliser (DPIA encore en cours)



EXEMPLE FIL ROUGE

Les écarts deviennent un **plan d'action concret sur 30 jours**, nourri par l'auto-réflexion et les recommandations de gouvernance.

PAGE 3/5

5 PRIORISATION DES ACTIONS

PRIORITÉ	DOMAINE CONCERNÉ	ACTION CLÉ	EFFORT (1-5)	IMPACT (1-5)
1	Données	Classification + monitoring de fraîcheur des flux catalogue	3	5
2	Compétences & culture	Former un binôme DDAO + monter l'équipe SAV en compétence	2	4
3	Sécurité & conformité	Finaliser le DPIA AI Act de l'agent Margaux	2	4

EFFORT 1 qq heures, sans budget · 2 qq jours, en interne · 3 qq semaines, budget limité · 4 plusieurs mois / prestataire · 5 chantier pluri-trimestriel

IMPACT 1 cosmétique · 2 gain limité · 3 gain réel sur un domaine clé · 4 gain structurant pluri-domaines · 5 déverrouille conformité / souveraineté

→ Prioriser Impact fort × Effort faible (quick wins), puis les chantiers à fort impact.

6 PLAN D'ACTION 30 JOURS

SEMAINE	ACTIONS À RÉALISER	LIVRABLE ATTENDU	RESPONSABLE
S1 - Analyse & cadrage	Cartographier les flux de données ; nommer le binôme DDAO	Cartographie des flux + rôles	C. Roussel
S2 - Conception	Concevoir le monitoring de fraîcheur + plan de formation	Specs monitoring + plan formation	IT / Ops
S3 - Mise en œuvre	Déployer le monitoring ; 1re session de formation équipe	Monitoring en prod · équipe formée	IT / Ops · C. Roussel
S4 - Contrôle & ajustement	Re-mesurer la maturité (audit flash) et ajuster	Audit flash · maturité cible 3,3	C. Roussel



EXEMPLE FIL ROUGE

L'audit se clôt par une **synthèse exécutive**, sa **validation** par le DDAO et la planification du **prochain audit**.

PAGE 4/5

7 ? QUESTIONS D'AUTO-RÉFLEXION

Quelle est la principale force de notre gouvernance agentique ?

La discipline de supervision : kill switch armé, registre tenu, revue hebdomadaire.

Quel est le plus grand risque non maîtrisé ?

La fraîcheur des données catalogue - cause directe de l'incident #4.

Quelles décisions doivent être prises en priorité ?

Industrialiser le monitoring des données et élargir le binôme DDAO pour réduire la dépendance individuelle.

8 ✓ RECOMMANDATIONS GÉNÉRALES

- ✓ Définir un cadre de gouvernance clair et approuvé
- ✓ Tenir un registre des agents et de leurs cas d'usage
- ✓ Renforcer la sécurité et la conformité (DPO, DPIA)
- Former et sensibiliser les équipes
- ✓ Nommer un responsable de gouvernance (DDAO)
- Standardiser la gestion et la classification des données
- ✓ Déployer des outils de supervision et d'alerte
- ✓ Mesurer régulièrement la performance et les risques

9 📄 SYNTHÈSE EXÉCUTIVE

PRINCIPALES CONCLUSIONS

Gouvernance Réactive (2,9/5) : supervision déjà mature, mais gouvernance des données et compétences à renforcer. L'incident #4 a validé les réflexes de contrôle et révélé l'angle mort « données ».

PRIORITÉS PRINCIPALES (1 À 5)

- 1 Monitoring de fraîcheur des données
- 2 Binôme DDAO + formation de l'équipe
- 3 DPIA AI Act de l'agent Margaux
- 4 Tableau de bord temps réel
- 5 Classification standardisée des données

BÉNÉFICES ATTENDUS

Réduire le risque d'incident données, sécuriser la continuité (moins de dépendance individuelle), viser une maturité « Défini » (3,3) au prochain audit.

PROCHAINES ÉTAPES IMMÉDIATES

Lancer le plan 30 jours dès le 11/06 ; planifier l'audit flash au 10/07/2026.



EXEMPLE FIL ROUGE

L'audit se clôt par une **synthèse exécutive**, sa **validation** par le DDAO et la planification du **prochain audit**.

PAGE 5/5

10

VALIDATION DE L'AUDIT

AUDITEUR

Camille Roussel

FONCTION

DDAO · Dir. transfo.
digitale

DATE

10/06/2026

VISA

C. R. ✓

11



PROCHAIN AUDIT

DATE RECOMMANDÉE

10/07/2026 (audit flash) puis 10/09/2026 (complet)

FRÉQUENCE RECOMMANDÉE

Trimestrielle

Semestrielle

Annuelle

Ponctuelle

✓ BONNES PRATIQUES

- ✓ Impliquer les parties prenantes clés dans l'audit
- ✓ S'appuyer sur des preuves, pas des impressions
- ✓ Évaluer chaque domaine indépendamment
- ✓ Prioriser les actions à fort impact

⚠ POINTS DE VIGILANCE

- ! Négliger la qualité des données
- ! Sous-estimer la sécurité et la conformité
- ! Manquer de visibilité sur les agents en production
- ! Un audit sans plan d'action concret

Et ensuite : décliner les actions dans un **plan ACF-10**, mettre à jour le **mandat ACF-13**, tracer les décisions au **registre ACF-09** et re-mesurer la souveraineté avec l'**ACF-01**.