



EXEMPLE FIL ROUGE

Deux jours après l'audit **ACF-11**, **Lendari** cartographie les risques de l'agent « Margaux » et de sa chaîne de données. Évaluation conduite par **Camille Roussel** (DDAO).

PAGE 1/4

1 INFORMATIONS GÉNÉRALES

ORGANISATION

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

ENTITÉ / DÉPARTEMENT

Transformation digitale / SAV

RESPONSABLE DE L'ÉVALUATION

Camille Roussel (DDAO)

DATE · PÉRIMÈTRE ÉVALUÉ

12/06/2026 - Agent « Margaux » (SAV & retours niv.1) + chaîne de données associée

AGENTS / SYSTÈMES CONCERNÉS

Agent Margaux (N2) · base retours/remboursements · intégration plateforme e-commerce

2 MATRICE DE RISQUE

Chaque risque est positionné selon sa **probabilité** (lignes, 5→1) et sa **gravité** (colonnes, 1→5). Le **score** = Probabilité × Gravité (1 à 25). Les pastilles indiquent où se placent les risques de Lendari.

ÉCHELLE DE COTATION - COMMENT CHOISIR P ET G (1 À 5)

NIV.	PROBABILITÉ (P) - QUE LE RISQUE SURVIENNE	GRAVITÉ (G) - IMPACT SI LE RISQUE SURVIENT
1	Très faible - quasi jamais (< 5 %/an), aucun précédent.	Mineur - négligeable, corrigé en routine.
2	Faible - peu probable (~5–20 %), rare sur plusieurs années.	Modéré - gêne limitée, coût/retard modéré, peu d'utilisateurs.
3	Modérée - possible (~20–50 %), quelques fois par an.	Sérieux - perturbation réelle, perte sensible, non-conformité mineure.
4	Élevée - probable (~50–80 %), récurrent / near-miss déjà vus.	Majeur - préjudice important, utilisateurs lésés en masse, manquement réglementaire signalable.
5	Très élevée - quasi-certain (> 80 %), déjà survenu / fréquent.	Critique - préjudice massif, sanction AI Act/RGPD, atteinte durable.

Échelle indicative - adaptez les seuils (% , montants) à votre contexte. Le score **P × G** se lit ensuite dans la matrice.

		GRAVITÉ (IMPACT) →				
		1 MINEUR	2 MODÉRÉ	3 SÉRIEUX	4 MAJEUR	5 CRITIQUE
PROB. ↓	5 TRÈS ÉLEVÉE	5	10	15	20	25
	4 ÉLEVÉE	4	8	12	16	20 R1
	3 MODÉRÉE	3	6	9 R5	12 R3·R4	15
	2 FAIBLE	2	4	6 R7	8 R2·R6	10
	1 TRÈS FAIBLE	1	2	3	4	5



EXEMPLE FIL ROUGE

Lendari inventorie **7 risques**, les note Probabilité × Gravité, puis isole les risques majeurs et leurs causes.

PAGE 2/4

3 INVENTAIRE DES RISQUES

Comment coter : 1 Probabilité P (1–5) 2 Gravité G (1–5) 3 Score = P × G
4 Niveau : 1–5 Faible · 6–12 Modéré · 13–19 Élevé · 20–25 Critique - définitions de P et G : [échelle p. 1](#).

ID	DESCRIPTION DU RISQUE (CAUSE / SCÉNARIO)	CATÉGORIE	P	G	SCORE	NIVEAU	CONTRÔLES EXISTANTS
R1	Désynchronisation des données de remboursement	Données	4	5	20	CRITIQUE	Cause racine incident #4 · monitoring en cours (ACF-10)
R2	Remboursement au-delà du plafond 100 €	Supervision & contrôle	2	4	8	MODÉRÉ	Cap dur 100 € · revue hebdo (ACF-09)
R3	Savoir concentré sur 2 personnes	Compétences & culture	3	4	12		Binôme DDAO en cours (ACF-10)
R4	DPIA / AI Act de Margaux non formalisée	Sécurité & conformité	3	4	12	MODÉRÉ	DPIA planifiée S3 (plan ACF-11)
R5	Réponse SAV inappropriée (ton, hallucination)	Technologie	3	3	9		Supervision quotidienne S1 · garde-fou ton
R6	Détection d'incident a posteriori (pas de temps réel)	Supervision & contrôle	2	4	8	MODÉRÉ	Kill switch > 2 % erreur, mais détection différée
R7	Drift du modèle après mise à jour fournisseur	Technologie	2	3	6		Tests de non-régression avant déploiement

Catégories = les 8 domaines ACF (mêmes que l'audit ACF-11).

4 ANALYSE DES RISQUES MAJEURS

TOP 5 DES RISQUES LES PLUS ÉLEVÉS

- 1 R1 - Désynchronisation des données (20 · Critique)
- 2 R3 - Dépendance à 2 personnes (12 · Modéré)
- 3 R4 - DPIA / AI Act non formalisée (12 · Modéré)
- 4 R5 - Réponse SAV inappropriée (9 · Modéré)
- 5 R2 / R6 - Plafond & détection différée (8 · Modéré)

PRINCIPALES CAUSES IDENTIFIÉES

- Données de remboursement non monitorées (cause de l'incident #4)
- Gouvernance jeune, concentrée sur deux personnes
- Conformité AI Act / DPIA non encore formalisée
- Détection d'incident différée - pas d'alerte temps réel



EXEMPLE FIL ROUGE

Chaque risque reçoit un **traitement selon son niveau**, décliné en un **plan d'action global priorisé**.

PAGE 3/4

5 TRAITEMENT & PRIORISATION PAR NIVEAU

NIVEAU DE RISQUE	PRIORITÉ	TRAITEMENT RECOMMANDÉ	EXEMPLES D'ACTIONS
CRITIQUE 20-25	P1	Traitement immédiat - risque inacceptable en l'état.	Suspendre ou restreindre l'agent · renforcer les contrôles · limiter le périmètre.
ÉLEVÉ 13-19	P2	Traitement prioritaire - réduction nécessaire.	Mesures d'atténuation · renforcer la supervision · plan d'action court terme.
MODÉRÉ 6-12	P3	Traitement planifié - acceptable sous conditions de contrôle.	Contrôles ciblés · surveillance active · réévaluation périodique.
FAIBLE 1-5	P4	Surveillance continue - risque maîtrisé.	Maintenir les contrôles existants · surveillance régulière · réévaluation.

6 PLAN D'ACTION GLOBAL

PRIO.	RISQUE PRINCIPAL	NIVEAU	ACTION CLÉ	ÉCHÉANCE	STATUT	RESPONSABLE
1	R1 - Désync. données remboursement	CRIT.	Déployer le monitoring de fraîcheur + classification	30/06/2026	EN COURS	C. Roussel
2	R3 - Dépendance à 2 personnes	MOD.	Constituer un binôme DDAO + plan de formation	15/07/2026	À FAIRE	C. Roussel
3	R4 - DPIA / AI Act Margaux		Formaliser la DPIA + registre de conformité	15/07/2026	À FAIRE	P. Dubois
4	R5 - Réponse SAV inappropriée	MOD.	Garde-fou de ton + revue d'un échantillon hebdo	30/06/2026	EN COURS	L. Fontaine
5	R6 - Détection a posteriori		Mettre en place une alerte temps réel du taux d'erreur	31/07/2026	À FAIRE	C. Roussel

✓ BONNES PRATIQUES

- ✓ Traiter d'abord les risques critiques et élevés
- ✓ Être factuel et s'appuyer sur des données
- ✓ Documenter toutes les décisions et hypothèses

⚠ POINTS DE VIGILANCE

- ! Ne pas sous-estimer les risques données et sécurité
- ! Inclure les risques éthiques, juridiques et réputationnels
- ! Ne pas confondre risque brut et risque résiduel



EXEMPLE FIL ROUGE

L'évaluation se clôt par le **suivi**, les **indicateurs clés**, une **synthèse** et sa **validation** par le DDAO.

PAGE 4/4

7 SUIVI & RÉÉVALUATION

FRÉQUENCE DE RÉÉVALUATION

Mensuelle

Trimestrielle

Semestrielle

Selon événement

PROCHAINE RÉÉVALUATION PRÉVUE LE

12/09/2026 (ou plus tôt si déclencheur)

DÉCLENCHEURS & MÉTHODES

- **Déclencheurs** : changement majeur de l'agent ou de son environnement · nouvel incident ou faille · évolution réglementaire (AI Act).
- **Méthodes** : revue des contrôles · analyse des incidents · consultation des parties prenantes · tests & audit.

8 INDICATEURS CLÉS

7

RISQUES IDENTIFIÉS

14 %

CRITIQUES + ÉLEVÉS

29 %

EN TRAITEMENT

5

RISQUES OUVERTS

25 j

DÉLAI MOYEN

9 SYNTHÈSE & RAPPORT

CONCLUSIONS PRINCIPALES

Un seul risque critique (désynchronisation des données - cause de l'incident #4), déjà en traitement. Six risques modérés sous contrôle. Profil cohérent avec la maturité « Réactif » (ACF-11).

RECOMMANDATIONS CLÉS (PRIORITÉS)

- 1 Monitoring de fraîcheur des données
- 2 Binôme DDAO + formation
- 3 DPIA AI Act de Margaux
- 4 Alerte temps réel du taux d'erreur
- 5 Tests de non-régression du modèle

BÉNÉFICES ATTENDUS DE LA GESTION DES RISQUES

Réduire le risque résiduel, sécuriser la conformité AI Act, renforcer la résilience humaine (moins de dépendance individuelle) et détecter les incidents plus tôt.

10 VALIDATION

VALIDATEUR

Camille Roussel

FONCTION

DDAO · Dir. transfo.
digitale

DATE

12/06/2026

SIGNATURE

C. R. ✓

Et ensuite : alimenter le **plan d'action ACF-10**, tracer les décisions au **registre ACF-09**, vérifier le **kill switch ACF-07**, mettre à jour le **mandat ACF-13** et reboucler avec l'audit **ACF-11**.