



EXEMPLE FIL ROUGE

Deux jours après l'audit **ACF-11**, **Rhena** cartographie les risques de l'agent « ANNA » et de sa chaîne de données. Évaluation conduite par **Dr Katrin Ostermann** (DDAO).

PAGE 1/4

1 INFORMATIONS GÉNÉRALES

ORGANISATION

Rhena - assurance (75 Md€)

ENTITÉ / DÉPARTEMENT

Conformité / pôle habitation

RESPONSABLE DE L'ÉVALUATION

Dr Katrin Ostermann (DDAO)

DATE · PÉRIMÈTRE ÉVALUÉ

02/10/2027 - Agent « ANNA » (sinistres habitation
niv.1) + chaîne de données associée

AGENTS / SYSTÈMES CONCERNÉS

Agent ANNA (N2) · barème de vétusté versionné ·
référentiel contrats

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 Rhena.

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) →				
PROB. ↓		1 MINEUR	2 MODÉRÉ	3 SÉRIeux	4 MAJEUR	5 CRITIQUE
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

Rhena 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	Barème non synchronisé avec la révision tarifaire	Données	4	5	20	CRITIQUE	Cause racine incident #4 · monitoring en cours (ACF-10)
R2	Indemnité au-delà du plafond 2 500 €	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	Biais par code postal non établi	Sécurité & conformité	3	4	12	MODÉRÉ	DPIA planifiée S3 (plan ACF-11)
R5	Réponse inappropriée à un assuré (ton, hallucination)	Technologie	3	3	9		Supervision quotidienne S1 · garde-fou ton
R6	Autorité d'arrêt non étendue à la filiale	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 - Barème non synchronisé (20 · Critique)
- 2 R3 - Dépendance à 2 personnes (12 · Modéré)
- 3 R4 - Biais par code postal non établi (12 · Modéré)
- 4 R5 - Réponse inappropriée à un assuré (9 · Modéré)
- 5 R2 / R6 - Plafond & arrêt non étendu (8 · Modéré)

PRINCIPALES CAUSES IDENTIFIÉES

- Barème non rapproché de la chaîne tarifaire (cause de l'incident #4)
- Gouvernance jeune, concentrée sur deux personnes
- Absence de biais non établie, donc non exclue
- Arrêt limité à l'Europe - la filiale n'est pas couverte



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 - Barème non synchronisé	CRIT.	Journaliser la version du barème + rapprochement tarifaire	31/03/2027	EN COURS	K. Ostermann
2	R3 - Dépendance à 2 personnes	MOD.	Constituer un binôme DDAO + plan de formation	31/12/2027	À FAIRE	K. Ostermann
3	R4 - Biais par code postal		Étude de biais + registre de conformité	15/01/2028	À FAIRE	S. Lindqvist
4	R5 - Réponse inappropriée	MOD.	Garde-fou de ton + revue d'un échantillon hebdo	31/10/2027	EN COURS	I. Baumgartner
5	R6 - Arrêt non étendu		Étendre l'autorité d'arrêt aux deux entités	30/04/2027	À FAIRE	K. Ostermann

✓ 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



7 SUIVI & RÉÉVALUATION

FRÉQUENCE DE RÉÉVALUATION

Mensuelle

Trimestrielle

Semestrielle

Selon événement

PROCHAINE RÉÉVALUATION PRÉVUE LE

02/01/2028 (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 (barème non synchronisé - cause de l'incident #4), déjà traité. Six risques modérés sous contrôle. Profil cohérent avec la maturité « Réactif » (ACF-11).

RECOMMANDATIONS CLÉS (PRIORITÉS)

- 1 Journal des versions de barème
- 2 Binôme DDAO + formation
- 3 Étude de biais par code postal
- 4 Autorité d'arrêt sur les deux entités
- 5 Tests de non-régression du modèle

BÉNÉFICES ATTENDUS DE LA GESTION DES RISQUES

Réduire le risque résiduel, établir l'absence de biais, renforcer la résilience humaine (moins de dépendance individuelle) et couper partout en même temps.

10 VALIDATION

VALIDATEUR

Dr Katrin Ostermann

FONCTION

DDAO · Dir. conformité

DATE

02/10/2027

SIGNATURE

K. O. ✓

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**.