



EXEMPLE FIL ROUGE

Six mois après le déploiement d'« ANNA » et l'**incident #4**, Rhena mesure la maturité de sa gouvernance agentique. Audit conduit par **Dr Katrin Ostermann** (DDAO).

PAGE 1/5

1 INFORMATIONS GÉNÉRALES

ORGANISATION

Rhena - assurance (75 Md€,
62 000 salariés)

RESPONSABLE DE L'AUDIT

Dr Katrin Ostermann (DDAO)

DATE DE L'AUDIT

30/09/2027

PÉRIMÈTRE ÉVALUÉ

Agent « ANNA » (sinistres habitation niv.1) + cadre de
gouvernance Rhena

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	Barème versionné depuis le 31/03
Technologie	Architecture · outils · résilience	1 2 3 4 5	Arrêt ACF-07 · deux socles, un modèle
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	Escalade à 41 % · capacité non recalculée
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	Satisfaction 4,1 · erreur 0,9 % · délai 2 h 10

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) : **3,1 / 5** DÉFINI



EXEMPLE FIL ROUGE

Rhena lit son score (3,1 / 5 - Défini), identifie ses forces et ses écarts majeurs, puis priorise les actions.

PAGE 2/5

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

- ✓ Gouvernance mature (4/5) : DDAO, mandat signé, registre tenu
- ✓ Indicateurs de qualité tous tenus (4/5) : erreur, délai, satisfaction
- ✓ Réflexe incident éprouvé - Europe coupée en 3 min

⚠ FAIBLESSES / ÉCARTS MAJEURS

- ! Supervision dépassée (3/5) - escalade à 41 % pour une cible de 35 %
- ! Compétences concentrées sur 2 personnes : risque de continuité
- ! Biais par code postal non établi, donc non exclu (ACF-P15)



5 ≡ PRIORISATION DES ACTIONS

PRIORITÉ	DOMAINE CONCERNÉ	ACTION CLÉ	EFFORT (1-5)	IMPACT (1-5)
1	Supervision	Recalculer la capacité de reprise et resserrer le périmètre	3	5
2	Compétences & culture	Former un binôme DDAO + monter le pôle habitation en compétence	2	4
3	Sécurité & conformité	Établir l'absence de biais par code postal (ACF-P15)	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	Mesurer la charge réelle de reprise ; nommer le binôme DDAO	Charge mesurée + rôles	K. Ostermann
S2 - Conception	Resserrer le périmètre délégué + plan de formation	Périmètre révisé + plan formation	DSI / Ops
S3 - Mise en œuvre	Appliquer le nouveau périmètre ; 1re session de formation	Périmètre en prod · équipe formée	DSI / Ops · K. Ostermann
S4 - Contrôle & ajustement	Re-mesurer la maturité (audit flash) et ajuster	Audit flash · maturité cible 3,5	K. Ostermann



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 ?

Le cadre écrit : DDAO nommée, mandat signé, registre tenu, arrêt éprouvé.

Quel est le plus grand risque non maîtrisé ?

La charge de supervision : 672 dossiers repris par jour pour une capacité de 492.

Quelles décisions doivent être prises en priorité ?

Resserrer le périmètre délégué 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 Définie (3,1/5) : cadre écrit et tenu, mais supervision dépassée 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 Capacité de supervision recalculée
- 2 Binôme DDAO + formation de l'équipe
- 3 Étude de biais par code postal
- 4 Tableau de bord temps réel
- 5 Périmètre délégué resserré

BÉNÉFICES ATTENDUS

Ramener l'escalade sous 35 %, sécuriser la continuité (moins de dépendance individuelle), viser une maturité « Défini » consolidée (3,5) au prochain audit.

PROCHAINES ÉTAPES IMMÉDIATES

Lancer le plan 30 jours dès le 01/10 ; planifier l'audit flash au 30/10/2027.



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

Dr Katrin Ostermann

FONCTION

DDAO · Dir. conformité

DATE

30/09/2027

VISA

K. O. ✓

11 PROCHAIN AUDIT

DATE RECOMMANDÉE

30/10/2027 (audit flash) puis 30/03/2028 (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**.