



RUNNING EXAMPLE

Two days after the **ACF-11** audit, **Rhena** maps the risks of agent "ANNA" and its data chain. Assessment led by **Dr Katrin Ostermann** (DDAO · Delegated Decision Agent Officer).

1 GENERAL INFORMATION

ORGANIZATION

Rhena · insurance (€75bn)

ENTITY / DEPARTMENT

Compliance / home claims unit

ASSESSMENT LEAD

Dr Katrin Ostermann (DDAO)

DATE · SCOPE ASSESSED

10/02/2027 : Agent "ANNA" (level 1 home claims) + associated data chain

AGENTS / SYSTEMS CONCERNED

Agent ANNA (N2) · versioned depreciation schedule · policy repository

2 RISK MATRIX

Each risk is positioned by its **probability** (rows, 5→1) and its **severity** (columns, 1→5). The **score** = Probability × Severity (1 to 25). The pins indicate where Rhena's risks fall.

SCORING SCALE · HOW TO CHOOSE P AND S (1 TO 5)

LVL.	PROBABILITY (P) · THAT THE RISK OCCURS	SEVERITY (S) · IMPACT IF THE RISK OCCURS
1	Very low · almost never (< 5 %/year), no precedent.	Minor · negligible, fixed as routine.
2	Low · unlikely (~5–20 %), rare over several years.	Moderate : limited disruption, modest cost/delay, few users.
3	Moderate · possible (~20–50 %), a few times per year.	Serious : real disruption, noticeable loss, minor non-compliance.
4	High : probable (~50–80 %), recurring / near-misses already observed.	Major : significant harm, large numbers of users affected, reportable regulatory breach.
5	Very high : near-certain (> 80 %), already occurred / frequent.	Critical : massive harm, AI Act/GDPR sanction, lasting damage.

Indicative scale : adapt the thresholds (% , amounts) to your context. The **P × S** score is then read in the matrix.

		SEVERITY (IMPACT) →				
PROB. ↓		1 MINOR	2 MODERATE	3 SERIOUS	4 MAJOR	5 CRITICAL
5 VERY HIGH		5	10	15	20	25
4 HIGH		4	8	12	16	20 R1
3 MODERATE		3	6	9 R5	12 R3·R4	15
2 LOW		2	4	6 R7	8 R2·R6	10
1 VERY LOW		1	2	3	4	5



RUNNING EXAMPLE

Rhena inventories **7 risks**, scores them Probability × Severity, then isolates the major risks and their root causes.

PAGE 2/4

3 RISK INVENTORY

How to score: 1 Probability P (1–5) 2 Severity S (1–5) 3 Score = P × S

4 Level: 1–5 Low · 6–12 Moderate · 13–19 High · 20–25 Critical · definitions of P and S: [scale p. 1](#).

ID	RISK DESCRIPTION (CAUSE / SCENARIO)	CATEGORY	P	S	SCORE	LEVEL	EXISTING CONTROLS
R1	Schedule out of sync with the tariff revision	Data	4	5	20	CRITICAL	Root cause of incident #4 · monitoring in progress (ACF-10)
R2	Settlement beyond the €2,500 cap	Supervision & control	2	4	8	MODERATE	Hard cap €100 · weekly review (ACF-09)
R3	Knowledge concentrated in 2 people	Skills & culture	3	4	12		DDAO pairing in progress (ACF-10)
R4	Bias by postcode not established	Security & compliance	3	4	12	MODERATE	DPIA scheduled S3 (ACF-11 plan)
R5	Inappropriate response to a policyholder (tone, hallucination)	Technology	3	3	9		Daily supervision S1 · tone guardrail
R6	Stop authority not extended to the subsidiary	Supervision & control	2	4	8	MODERATE	Kill switch > 2% error, but delayed detection
R7	Model drift after vendor update	Technology	2	3	6		Non-regression tests before deployment

Categories = the 8 ACF domains (same as the ACF-11 audit).

4 ANALYSIS OF MAJOR RISKS

TOP 5 HIGHEST RISKS

- 1 R1 · Schedule out of sync (20 · Critical)
- 2 R3 · Dependency on 2 people (12 · Moderate)
- 3 R4 · Bias by postcode not established (12 · Moderate)
- 4 R5 · Inappropriate response to a policyholder (9 · Moderate)
- 5 R2 / R6 · Cap & stop not extended (8 · Moderate)

MAIN ROOT CAUSES IDENTIFIED

- Schedule not tied to the tariff chain (cause of incident #4)
- Young governance, concentrated on two people
- Absence of bias not established, therefore not ruled out
- Stop limited to Europe · the subsidiary is not covered



RUNNING EXAMPLE

Each risk is given a **treatment according to its level**, broken down into a **prioritized global action plan**.

PAGE 3/4

5 TREATMENT & PRIORITIZATION BY LEVEL

RISK LEVEL	PRIORITY	RECOMMENDED TREATMENT	EXAMPLE ACTIONS
CRITICAL 20–25	P1	Immediate treatment · risk unacceptable as it stands.	Suspend or restrict the agent · strengthen controls · narrow the scope.
HIGH 13–19	P2	Priority treatment · reduction required.	Mitigation measures · strengthen supervision · short-term action plan.
MODERATE 6–12	P3	Planned treatment · acceptable subject to control conditions.	Targeted controls · active monitoring · periodic re-assessment.
LOW 1–5	P4	Ongoing monitoring · risk under control.	Maintain existing controls · regular monitoring · re-assessment.

6 GLOBAL ACTION PLAN

PRIO.	MAIN RISK	LEVEL	KEY ACTION	DEADLINE	STATUS	OWNER
1	R1 · Schedule out of sync	CRIT.	Log the schedule version + tariff reconciliation	03/31/2027	IN PROGRESS	K. Ostermann
2	R3 · Dependency on 2 people	MOD.	Establish DDAO pairing + training plan	12/31/2027	TO DO	K. Ostermann
3	R4 · Bias by postcode		Bias study + compliance registry	01/15/2028	TO DO	S. Lindqvist
4	R5 · Inappropriate response	MOD.	Tone guardrail + weekly sample review	10/31/2027	IN PROGRESS	I. Baumgartner
5	R6 · Stop not extended		Extend stop authority to both entities	04/30/2027	TO DO	K. Ostermann

✓ BEST PRACTICES

- ✓ Address critical and high risks first
- ✓ Be factual and rely on data
- ✓ Document all decisions and assumptions

⚠ WATCH-OUTS

- ! Do not underestimate data and security risks
- ! Include ethical, legal and reputational risks
- ! Do not confuse inherent risk with residual risk



RUNNING EXAMPLE

The assessment closes with **monitoring**, **key indicators**, a **summary** and its **validation** by the DDAO.

PAGE 4/4

7 MONITORING & RE-ASSESSMENT

RE-ASSESSMENT FREQUENCY

Monthly

Quarterly

Semi-annually

Event-driven

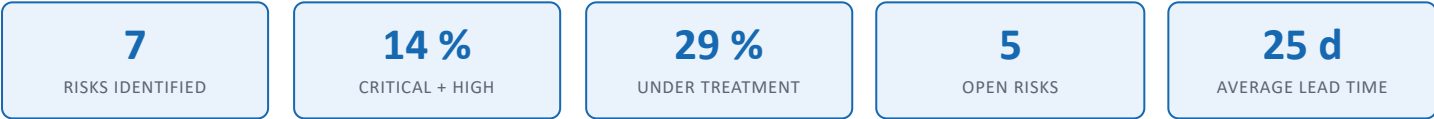
NEXT RE-ASSESSMENT SCHEDULED FOR

01/02/2028 (or earlier if triggered)

TRIGGERS & METHODS

- **Triggers:** major change to the agent or its environment · new incident or vulnerability · regulatory evolution (AI Act).
- **Methods:** review of controls · incident analysis · stakeholder consultation · tests & audit.

8 KEY INDICATORS



9 SUMMARY & REPORT

MAIN CONCLUSIONS

A single critical risk (schedule out of sync · cause of incident #4), already treated. Six moderate risks under control. Profile consistent with the "Defined" maturity (ACF-11).

KEY RECOMMENDATIONS (PRIORITIES)

- 1 Schedule version log
- 2 DDAO pairing + training
- 3 Bias study by postcode
- 4 Stop authority across both entities
- 5 Model non-regression tests

EXPECTED BENEFITS OF RISK MANAGEMENT

Reduce residual risk, establish the absence of bias, strengthen human resilience (less individual dependency) and cut off everywhere at once.

10 VALIDATION

VALIDATOR Dr Katrin Ostermann	ROLE DDAO · Chief Compliance Officer	DATE 10/02/2027	SIGNATURE K. O. ✓
----------------------------------	---	--------------------	----------------------

Next steps: feed the **ACF-10 action plan**, log decisions in the **ACF-09 registry**, verify the **ACF-07 kill switch**, update the **ACF-13 mandate** and loop back to the **ACF-11 audit**.