



RUNNING EXAMPLE

Six months after deploying "ANNA" and **incident #4, Rhena** measures the maturity of its agentic governance. Audit conducted by **Dr Katrin Ostermann** (DDAO · Delegated Decision Agent Officer).

1 GENERAL INFORMATION

ORGANIZATION

Rhena · insurance (€75bn)

AUDIT LEAD

Dr Katrin Ostermann (DDAO)

AUDIT DATE

09/30/2027

SCOPE ASSESSED

Agent "ANNA" (level 1 home claims) + Rhena governance framework

AUDIT OBJECTIVE

Measure post-incident #4 maturity and frame a 30-day plan of priority actions

2 AUDIT GRID · MATURITY ACROSS 8 DOMAINS

DOMAIN ASSESSED	KEY CRITERIA	MATURITY (1 TO 5)	EVIDENCE / COMMENT
Governance	Framework defined · clear roles	1 2 3 4 5	Constitution v1.0 · DDAO · committee
Strategy & alignment	Alignment · objectives by use case	1 2 3 4 5	ACF-13 Mandate · KPIs (ACF-06)
Data	Quality · classification · GDPR	1 2 3 4 5	Schedule versioned since 03/31
Technology	Architecture · tools · resilience	1 2 3 4 5	Stop ACF-07 · two platforms, one model
Security & compliance	Security · AI Act · risk management	1 2 3 4 5	DPO · GDPR up to date · DPIA in progress
Supervision & control	Monitoring · alerts · kill switch	1 2 3 4 5	Escalation at 41% · capacity not recomputed
Skills & culture	Skills · training · culture	1 2 3 4 5	Know-how held by 2 people · no training
Performance & value	Metrics · value · improvement	1 2 3 4 5	Satisfaction 4.1 · error 0.9% · time 2h10

1 Initial · ad hoc 2 Reactive · loosely formalized 3 Defined · documented 4 Managed · measured & controlled
5 Optimal · optimized & innovative

Overall maturity level (average of 8 domains): 3.1 / 5 DEFINED



RUNNING EXAMPLE

Rhena reads its score (3.1 / 5 · Defined), identifies its strengths and major gaps, then prioritizes actions.

PAGE 2/5

3 SCORE INTERPRETATION

AVERAGE SCORE	LEVEL	INTERPRETATION	RECOMMENDED ACTIONS
1.0 – 1.9	INITIAL	Governance nonexistent or very weak. High risks, insufficient control.	Lay the foundations: framework, roles, basic policies, awareness.
2.0 – 2.9	REACTIVE	Approach underway but unstructured. Significant vulnerabilities.	Formalize key processes, document and strengthen controls.
3.0 – 3.9	DEFINED	Governance in place but improvable. Consistency to be enhanced.	Strengthen measurement, supervision, and strategic alignment.
4.0 – 4.4	MANAGED	Robust and measured governance. Strong risk control.	Optimize effectiveness and value. Automate certain controls.
4.5 – 5.0	OPTIMAL	Benchmark governance. Continuous improvement culture.	Innovate, share best practices, aim for excellence.

4 RESULTS ANALYSIS

✓ IDENTIFIED STRENGTHS

- ✓ Mature governance (4/5): DDAO, signed mandate, register maintained
- ✓ All quality indicators met (4/5): error, time, satisfaction
- ✓ Proven incident response · Europe cut off in 3 min

⚠ WEAKNESSES / MAJOR GAPS

- ! Supervision overrun (3/5) · escalation at 41% against a 35% target
- ! Skills concentrated in 2 people: business continuity risk
- ! Bias by postcode not established, therefore not ruled out (ACF-P15)



RUNNING EXAMPLE

Gaps become a **concrete 30-day action plan**, fueled by self-reflection and governance recommendations.

5 ACTION PRIORITIZATION

PRIORITY	DOMAIN CONCERNED	KEY ACTION	EFFORT (1-5)	IMPACT (1-5)
1	Supervision	Recompute rework capacity and tighten the perimeter	3	5
2	Skills & culture	Train a DDAO pair + upskill the home claims unit	2	4
3	Security & compliance	Establish the absence of bias by postcode (ACF-P15)	2	4

EFFORT 1 a few hours, no budget · 2 a few days, in-house · 3 a few weeks, limited budget · 4 several months / external provider · 5 multi-quarter initiative

IMPACT 1 cosmetic · 2 limited gain · 3 real gain in one key domain · 4 structural gain across multiple domains · 5 unlocks compliance / sovereignty

→ Prioritize High Impact × Low Effort (quick wins), then high-impact initiatives.

6 30-DAY ACTION PLAN

WEEK	ACTIONS TO COMPLETE	EXPECTED DELIVERABLE	OWNER
W1 · Analysis & scoping	Measure real rework load; appoint the DDAO pair	Measured load + roles	K. Ostermann
W2 · Design	Tighten the delegated perimeter + training plan	Revised perimeter + training plan	IT / Ops
W3 · Implementation	Apply the new perimeter; 1st training session	Perimeter in production · team trained	IT / Ops · K. Ostermann
W4 · Control & adjustment	Re-measure maturity (flash audit) and adjust	Flash audit · target maturity 3.5	K. Ostermann



RUNNING EXAMPLE

The audit closes with an **executive summary**, its **validation** by the DDAO, and the scheduling of the **next audit**.

PAGE 4/5

7 ? SELF-REFLECTION QUESTIONS

What is the primary strength of our agentic governance?

The written framework: DDAO appointed, mandate signed, register maintained, stop tested.

What is the greatest uncontrolled risk?

Supervision load: 672 files reworked a day against a capacity of 492.

Which decisions must be made first?

Tighten the delegated perimeter and expand the DDAO pair to reduce individual dependency.

8 ✓ GENERAL RECOMMENDATIONS

- ☒ Define a clear, approved governance framework
- ☒ Maintain a register of agents and their use cases
- ☒ Strengthen security and compliance (DPO, DPIA)
- ☐ Train and raise team awareness
- ☒ Appoint a governance lead (DDAO)
- ☐ Standardize data management and classification
- ☒ Deploy supervision and alerting tools
- ☒ Measure performance and risks regularly

9 📄 EXECUTIVE SUMMARY

KEY FINDINGS

Governance is Defined (3.1/5): the framework is written and kept, but supervision is overrun and skills must be strengthened. Incident #4 validated control reflexes and exposed the "data" blind spot.

TOP PRIORITIES (1 TO 5)

- 1 Supervision capacity recomputed
- 2 DDAO pair + team training
- 3 Bias study by postcode
- 4 Real-time dashboard
- 5 Delegated perimeter tightened

EXPECTED BENEFITS

Bring escalation below 35%, secure business continuity (less individual dependency), aim for a consolidated "Defined" maturity (3.5) at the next audit.

IMMEDIATE NEXT STEPS

Launch the 30-day plan starting 10/01; schedule the flash audit for 10/30/2027.



30-DAY GOVERNANCE AUDIT

*Assess the maturity of your agentic governance
and build a 30-day action plan*

LEVEL	Operational
DURATION	1 - 1.5 days
USE	Self-diagnostic / audit
TRACK	Toolkit

RUNNING EXAMPLE

The audit closes with an **executive summary**, its **validation** by the DDAO, and the scheduling of the **next audit**.

PAGE 5/5

10



AUDIT VALIDATION

AUDITOR

Dr Katrin Ostermann

ROLE

DDAO · Chief
Compliance Officer

DATE

09/30/2027

SIGN-OFF

K. O. ✓

11



NEXT AUDIT

RECOMMENDED DATE

10/30/2027 (flash audit) then 03/30/2028 (full)

RECOMMENDED FREQUENCY

Quarterly

Semi-annual

Annual

Ad hoc

✓ BEST PRACTICES

- ✓ Involve key stakeholders in the audit
- ✓ Rely on evidence, not impressions
- ✓ Assess each domain independently
- ✓ Prioritize high-impact actions

⚠ WATCH POINTS

- ! Neglecting data quality
- ! Underestimating security and compliance
- ! Lacking visibility into agents in production
- ! An audit without a concrete action plan

What's next: translate actions into an **ACF-10 plan**, update the **ACF-13 Mandate**, log decisions in the **ACF-09 register**, and re-measure sovereignty with **ACF-01**.