



RUNNING EXAMPLE

Two days after the **ACF-10** audit, **Lendari** maps the risks of agent "Margaux" and its data chain.
Assessment led by **Camille Roussel** (DDAO — Delegated Decision Agent Officer).

OBJECTIVE

Identify, assess and prioritize the risks of your AI agents. Each risk is scored **Probability × Severity** (score 1→25), then assigned to one of the **8 ACF domains** (the same categories as the **ACF-10** audit) to build a prioritized treatment plan.

1 GENERAL INFORMATION

ORGANIZATION

Lendari — fashion e-commerce
(€120M, 90 employees)

ENTITY / DEPARTMENT

Digital transformation /
Customer service

ASSESSMENT LEAD

Camille Roussel (DDAO)

DATE · SCOPE ASSESSED

06/12/2026 — Agent "Margaux" (Tier-1 customer
service & returns) + associated data chain

AGENTS / SYSTEMS CONCERNED

Agent Margaux (N2) · returns/refunds database · e-commerce platform integration

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 Lendari'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

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

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	Refund data desynchronization	Data	4	5	20	CRITICAL	Root cause of incident #4 · monitoring in progress (ACF-09)
R2	Refund beyond the €100 cap	Supervision & control	2	4	8	MODERATE	Hard cap €100 · weekly review (ACF-08)
R3	Knowledge concentrated in 2 people	Skills & culture	3	4	12		DDAO pairing in progress (ACF-09)
R4	DPIA / AI Act for Margaux not formalized	Security & compliance	3	4	12	MODERATE	DPIA scheduled S3 (ACF-10 plan)
R5	Inappropriate customer service response (tone, hallucination)	Technology	3	3	9		Daily supervision S1 · tone guardrail
R6	Post-hoc incident detection (no real-time)	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-10 audit).

4 ANALYSIS OF MAJOR RISKS

TOP 5 HIGHEST RISKS

- 1 R1 — Data desynchronization (20 · Critical)
- 2 R3 — Dependency on 2 people (12 · Moderate)
- 3 R4 — DPIA / AI Act not formalized (12 · Moderate)
- 4 R5 — Inappropriate customer service response (9 · Moderate)
- 5 R2 / R6 — Cap & delayed detection (8 · Moderate)

MAIN ROOT CAUSES IDENTIFIED

- Refund data not monitored (cause of incident #4)
- Young governance, concentrated on two people
- AI Act / DPIA compliance not yet formalized
- Delayed incident detection — no real-time alerting



RUNNING EXAMPLE

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

5 TREATMENT & PRIORITIZATION BY LEVEL

RISK LEVEL	PRIORITY	RECOMMENDED TREATMENT	EXAMPLE ACTIONS
<div>CRITICAL</div> <div>20–25</div>	P1	Immediate treatment — risk unacceptable as it stands.	Suspend or restrict the agent · strengthen controls · narrow the scope.
<div>HIGH</div> <div>13–19</div>	P2	Priority treatment — reduction required.	Mitigation measures · strengthen supervision · short-term action plan.
<div>MODERATE</div> <div>6–12</div>	P3	Planned treatment — acceptable subject to control conditions.	Targeted controls · active monitoring · periodic re-assessment.
<div>LOW</div> <div>1–5</div>	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 — Refund data desync.	CRIT.	Deploy freshness monitoring + classification	06/30/2026	IN PROGRESS	C. Roussel
2	R3 — Dependency on 2 people	MOD.	Establish DDAO pairing + training plan	07/15/2026	TO DO	C. Roussel
3	R4 — DPIA / AI Act Margaux		Formalize the DPIA + compliance registry	07/15/2026	TO DO	K. Belkacem
4	R5 — Inappropriate customer service response	MOD.	Tone guardrail + weekly sample review	06/30/2026	IN PROGRESS	L. Fontaine
5	R6 — Post-hoc detection		Implement real-time alerting on error rate	07/31/2026	TO DO	C. Roussel

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

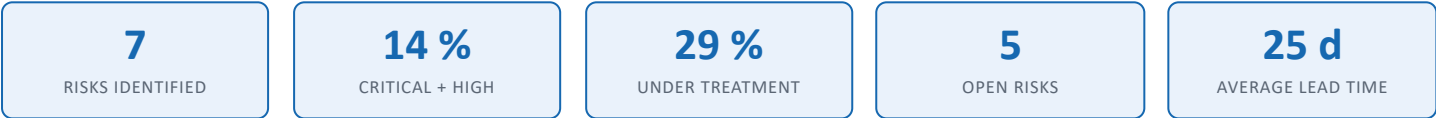
NEXT RE-ASSESSMENT SCHEDULED FOR

09/12/2026 (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 (data desynchronization — cause of incident #4), already under treatment. Six moderate risks under control. Profile consistent with the "Reactive" maturity (ACF-10).

KEY RECOMMENDATIONS (PRIORITIES)

- 1 Data freshness monitoring
- 2 DDAO pairing + training
- 3 DPIA AI Act for Margaux
- 4 Real-time error rate alerting
- 5 Model non-regression tests

EXPECTED BENEFITS OF RISK MANAGEMENT

Reduce residual risk, secure AI Act compliance, strengthen human resilience (less individual dependency) and detect incidents earlier.

10 VALIDATION

VALIDATOR Camille Roussel	ROLE DDAO · Director of digital transformation	DATE 06/12/2026	SIGNATURE C. R. ✓
------------------------------	---	--------------------	----------------------

Next steps: feed the **ACF-09 action plan**, log decisions in the **ACF-08 registry**, verify the **ACF-06 kill switch**, update the **ACF-12 mandate** and loop back to the **ACF-10 audit**.