# AGENTIC RISK ASSESSMENT

*Identify, assess and prioritize risks tied to your AI agents to control them more effectively*

| | |
|---|---|
| LEVEL | Operational |
| DURATION | 1 - 2 days |
| USE | Assessment / prioritization |
| TRACK | Toolkit |



**OBJECTIVE**

Identify, assess and prioritize the risks of your AI agents. Each risk is scored **Likelihood × Severity** (score 1→25), then assigned to one of the **8 ACF domains** (same categories as the **ACF-11** audit) in order to build a prioritized treatment plan.

## 1 GENERAL INFORMATION

ORGANIZATION

ENTITY / DEPARTMENT

ASSESSMENT LEAD

DATE · SCOPE ASSESSED

AGENTS / SYSTEMS COVERED

## 2 RISK MATRIX

Position each risk according to its **likelihood** (rows, 5→1) and its **severity** (columns, 1→5). The **score** = Likelihood × Severity (1 to 25). The cell color indicates the risk level (see legend).

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

| LVL. | LIKELIHOOD (L) · THAT THE RISK OCCURS | SEVERITY (S) · IMPACT IF THE RISK OCCURS |
|---|---|---|
| 1 | **Very low** · hardly ever (< 5 %/yr), no precedent. | **Minor** · negligible, fixed in routine operations. |
| 2 | **Low** : unlikely (~5–20 %), rare across several years. | **Moderate** : limited disruption, moderate cost/delay, few users affected. |
| 3 | **Moderate** · possible (~20–50 %), a few times a year. | **Serious** : real disruption, significant loss, minor non-compliance. |
| 4 | **High** : probable (~50–80 %), recurring / near-misses already observed. | **Major** : significant harm, large-scale user impact, reportable regulatory breach. |
| 5 | **Very high** : near-certain (> 80 %), already occurred / frequent. | **Critical** : massive harm, AI Act/GDPR sanction, lasting damage. |

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

SEVERITY (IMPACT) →

| LIK. ↓ | 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 |
| 3 MODERATE | 3 | 6 | 9 | 12 | 15 |
| 2 LOW | 2 | 4 | 6 | 8 | 10 |
| 1 VERY LOW | 1 | 2 | 3 | 4 | 5 |

**Critical** 20–25 · immediate action  **High** 13–19 · priority action  **Moderate** 6–12 · monitoring & plan  **Low** 1–5 · risk under control

# AGENTIC RISK ASSESSMENT

*Identify, assess and prioritize risks tied to your AI agents to control them more effectively*

| | |
|---|---|
| LEVEL | Operational |
| DURATION | 1 - 2 days |
| USE | Assessment / prioritization |
| TRACK | Toolkit |



## 3 ☰ RISK INVENTORY

**How to score:** 1 Likelihood **L** (1–5) 2 Severity **S** (1–5) 3 **Score = L × S**
4 Level: **1–5** Low · **6–12** Moderate · **13–19** High · **20–25** Critical · definitions of L and S: **scale p. 1**.

| ID | RISK DESCRIPTION (CAUSE / SCENARIO) | CATEGORY | L | S | SCORE | LEVEL | EXISTING CONTROLS |
|---|---|---|---|---|---|---|---|
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

**Categories** = the 8 ACF domains (same as the ACF-11 audit): Governance · Strategy & alignment · Data · Technology · Security & compliance · Oversight & control · Skills & culture · Performance & value.

## 4 ANALYSIS OF MAJOR RISKS

### TOP 5 HIGHEST RISKS

1.
2.
3.
4.
5.

### MAIN IDENTIFIED ROOT CAUSES

# AGENTIC RISK ASSESSMENT

*Identify, assess and prioritize risks tied to your AI agents to control them more effectively*

| | |
|---|---|
| LEVEL | Operational |
| DURATION | 1 - 2 days |
| USE | Assessment / prioritization |
| TRACK | Toolkit |



## 5 TREATMENT & PRIORITIZATION BY LEVEL

| RISK LEVEL | PRIORITY | RECOMMENDED TREATMENT | EXAMPLE ACTIONS |
|---|---|---|---|
| CRITICAL 20–25 | P1 | Immediate treatment · unacceptable risk in its current state. | Suspend or restrict the agent · strengthen controls · narrow scope. |
| HIGH 13–19 | P2 | Priority treatment · reduction required. | Mitigation measures · reinforce oversight · short-term action plan. |
| MODERATE 6–12 | P3 | Planned treatment · acceptable under control conditions. | Targeted controls · active monitoring · periodic reassessment. |
| LOW 1–5 | P4 | Continuous monitoring · risk under control. | Maintain existing controls · regular monitoring · reassessment. |

## 6 OVERALL ACTION PLAN

| PRIO. | MAIN RISK | LEVEL | KEY ACTION | DUE DATE | STATUS | OWNER |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

### BEST PRACTICES

- ✓ Address critical and high risks first
- ✓ Stay factual and rely on data
- ✓ Document every decision and assumption

### POINTS OF VIGILANCE

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

# AGENTIC RISK ASSESSMENT

*Identify, assess and prioritize risks tied to your AI agents to control them more effectively*

| | |
|---|---|
| LEVEL | Operational |
| DURATION | 1 - 2 days |
| USE | Assessment / prioritization |
| TRACK | Toolkit |



## 7 MONITORING & REASSESSMENT

### REASSESSMENT FREQUENCY

Monthly | Quarterly | Semiannual | Event-driven

### NEXT REASSESSMENT SCHEDULED FOR

### TRIGGERS & METHODS

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

## 8 KEY INDICATORS

| RISKS IDENTIFIED | CRITICAL + HIGH | UNDER TREATMENT | OPEN RISKS | AVERAGE LEAD TIME |
|---|---|---|---|---|
| | | | | |

## 9 SUMMARY & REPORT

### KEY CONCLUSIONS

### KEY RECOMMENDATIONS (PRIORITIES)

1.
2.
3.
4.
5.

### EXPECTED BENEFITS FROM RISK MANAGEMENT

## 10 VALIDATION

| VALIDATOR | ROLE | DATE | SIGNATURE |
|---|---|---|---|
| | | | |

**What's next:** feed the **ACF-10 action plan**, log decisions in the **ACF-09 register**, verify the **ACF-07 kill switch**, update the **ACF-13 mandate** and loop back with the **ACF-11** audit.