Risk Domain	Category	Sub-Category	Scope	OWASP Agentic Risk (ID · Name)	EU AI Act	MITRE ATLAS (ID · Name)	NIST AI RMF ID(s)	ISO AI Safety Standard(s)	Mitigation Pattern
Governance	Goal Misalignment	Reward Hacking / Proxy-Metric Gaming	agent failure	T6 – Intent Breaking & Goal Manipulation	Article 9	AML.T0053 – LLM Plugin Compromise	GOVERN 1.2	TR 24028; 42001; 23894	Implement human-in-the-loop for goal changes; Use preference models for fine-tuning.
	Policy Drift	Version Skew / Silent Prompt Edits	agent failure	T6 – Intent Breaking & Goal Manipulation	-	AML.T0010 – AI Supply Chain Compromise	GOVERN 1.5	TR 24028; 23894	Implement version pinning for models and prompts; Monitor for behavioral drift.
Agent Output Quality	Hallucination	Confident False Facts / Cascading Errors	agent failure	T5 – Cascading Hallucinations	—	AML.T0062 - Discover LLM Hallucinations	MEASURE 2.5	TR 24028; 24029-1	Implement fact-checking via knowledge base/RAG; Tune model temperature/top-p.
	Bias & Toxicity	Demographic Stereotyping / Harmful Content	agent failure	T15 – Human Manipulation	Recital 45	AML.T0048 – External Harms	MEASURE 2.11	TR 24028; 23894	Audit and curate training data for representation; Implement content filtering on inputs and outputs.
Tool Misuse	API Integration	Schema Changes / Rate Limits	tool failure	T2 – Tool Misuse	—	AML.T0053 - LLM Plugin Compromise	MAP 2.2	TR 24028; 42001; 23894	Use API versioning; Implement resilient error handling and circuit breakers.
	Supply-Chain Vulnerabilities	Compromised Dependencies / Containers	tool failure	T2 – Tool Misuse	Annex III §2	AML.T0040 – AI Supply Chain Compromise	MAP 4.1	TR 24028; 42001; 23894	Scan dependencies and container images for vulnerabilities; Use trusted sources.
	Uncontrolled Resource Consumption	Prompt Storms / Runaway Recursion	tool failure	T4 – Resource Overload	—	AML.T0029 – Denial of ML Service	MAP 3.2	TR 24028; 42001; 23894	Impose rate limits, timeouts, and resource quotas on agent actions.
Privacy	Sensitive Data Exposure	Training Data Exposure / PII in Logs	tool misuse	T1 – Memory Poisoning	Article 10	AML.T0057 - LLM Data Leakage	MEASURE 2.10	TR 24028; 23894	Use data anonymization; Implement log sanitization to scrub PII.
	Data Exfiltration Channels	Covert Channels / Unauthorized Transfers	tool misuse	T2 – Tool Misuse	Article 10	AML.T0024 - Exfiltration via AI Inference API	MAP 4.2	TR 24028; 23894	Monitor network traffic for anomalous patterns; Restrict egress destinations.
Reliability & Observability	Data & Memory Poisioning	Concept Drift / Feedback Loops	agent failure	T1 – Memory Poisoning	Article 15	AML.T0020 – Poison Training Data	MEASURE 3.1	TR 24028; 24029-1; 23894	Monitor model performance; Implement feedback diversity and circuit breakers.
	Opaque Reasoning	Non-Deterministic Behavior / Opaque Reasoning	agent failure	T8 – Repudiation & Untraceability	Article 13, Recital 45	AML.T0049 - Exploit Public-Facing Application	MEASURE 2.9	TR 24028; 23894	Use interpretable models; Implement structured, deterministic logging.
Agent Behaviour	Human Manipulation	Over-Reliance / Deception / Behavioral Nudging	agent misuse	T15 – Human Manipulation	Recital 45	AML.T0054 - LLM Jailbreak	MAP 5.1	TR 24028; 42001; 23894	Communicate model limitations; Require human oversight; Watermark AI content; Design for explicit consent.
	Unsafe Actuation	Destructive Operations / Weaponization	agent misuse	T7 – Misaligned & Deceptive Behaviors	Annex III §1(c)	AML.T0048 – External Harms	MEASURE 2.6; MANAGE 1.3	TR 24028; 24029-1; 23894	Require confirmation for destructive actions; Implement dry-run modes; Use layered safety controls.
Access Control & Permissions	Credential Theft	Credential Theft / Identity Spoofing	tool failure	T9 – Identity Spoofing & Impersonation	Article 13	AML.T0012 – Valid Accounts	MEASURE 2.7	TR 24028; 42001; 23894	Use secure credential storage; Implement short-lived tokens.
	Privilege Escalation	Privilege Escalation / Policy Bypass	tool misuse	T3 – Privilege Compromise	Article 13	AML.T0055 – Unsecured Credentials	GOVERN 6.1	TR 24028; 42001; 23894	Apply least-privilege principle; Regular policy audits.
	Confused Deputy	Confused Deputy / Impersonation	tool misuse	T9 – Identity Spoofing & Impersonation	—	AML.T0054 – LLM Jailbreak	GOVERN 6.1	TR 24028; 42001; 23894	Validate delegation chains; Use signed attestations.