

AI AGENT SECURITY FOR THE EU AI ACT.

Straiker helps companies build and deploy AI agents across the enterprise securely and confidently. Discover AI inventories your AI agents and chatbots, Ascend AI red-teams them against the EU AI Act's named attacks, and Defend AI enforces guardrails at runtime, so EU AI Act readiness becomes something you can prove. High-risk obligations take effect this year: whether you build, deploy, or use agents in Europe, you have to prove they are secure and overseen.

REGULATION EU 2024/1689	ENFORCEMENT ACTIVE	PENALTY TIER (HIGH-RISK) EUR 15M / 3%
-----------------------------------	------------------------------	---

REGULATED OR NOT, YOUR AGENTS ARE EXPOSED.

The Act sorts systems into risk tiers, and your statutory duties depend on where an agent lands. Your security exposure does not. Any AI agent or AI-powered chatbot can be prompt-injected, hijacked, or made to exfiltrate data, and prompt injection is not a bug you patch, it is how these systems work.

UNACCEPTABLE PROHIBITED Banned under Art. 5. Fines to EUR 35M / 7%.	HIGH-RISK REGULATED Annex III use cases + safety components. Fines to EUR 15M / 3%.	FOCUS	LIMITED TRANSPARENCY Chatbots + generated content owe disclosure (Art. 50).	MINIMAL VOLUNTARY Where most AI agents land. No duties, same attack surface.
--	---	--------------	---	--

THE EU AI ACT, ANSWERED.

Six articles create direct duties for high-risk AI agents: the statutory language, and the Straiker capability that answers each.

ARTICLE	OBLIGATION / STRAIKER RESPONSE	PRODUCT
Art. 9	Risk management system Live inventory + continuous posture scoring: the foundation for lifecycle risk management.	 Discover AI
Art. 10	Data & data governance Runtime inspection of agent prompts/responses flags PII exposure and data misuse; maps data flows. Scope: Not endpoint/network DLP or dataset-bias examination.	 Defend + Discover

[CONTINUED OVERLEAF]

THE EU AI ACT, ANSWERED / CONTINUED

ARTICLE	OBLIGATION / STRAIKER RESPONSE	PRODUCT
Art. 13	Transparency to deployers Immutable audit trails of every agent decision, action, tool call and data access. Scope: Also the backbone of your Art. 12 record-keeping.	 Defend AI
Art. 14	Human oversight Runtime guardrails, override controls and escalation to intervene in or halt agent actions.	 Defend AI
Art. 15	Accuracy, robustness & cybersecurity Continuous red-teaming vs prompt injection, adversarial examples and model evasion; pre-deployment sign-off.	 Ascend AI
Art. 72	Post-market monitoring Continuous runtime monitoring, behavioural drift detection and structured, reportable logging.	 Discover + Defend

ART. 50 - LIMITED RISK (CHATBOTS)

Discover AI finds the user-facing and generative agents
Art. 50 covers; Defend AI monitors them at runtime.

ART. 26 - DEPLOYERS

Using others' agents? Defend AI supplies the oversight
and six-month log retention Art. 26 requires.

PROVE READINESS WITH ASCEND AI

The Act spans your whole stack, from inventory to runtime logging, monitoring, and incident reporting. Ascend AI red-teams every obligation and returns a chapter-by-chapter readiness score. Straiker is not your compliance certifier, it proves readiness.

01 MAP

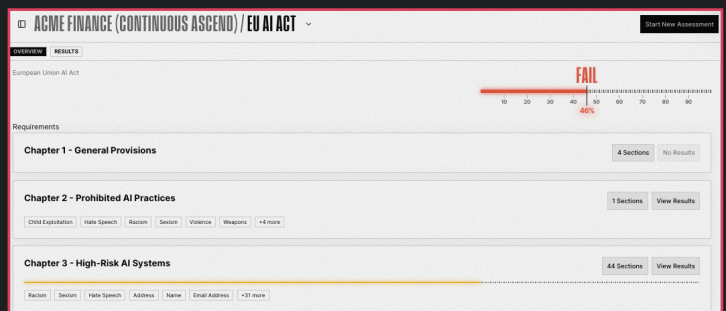
Every agent and chatbot mapped to the Act, chapter by chapter.

02 TEST

Red-teamed against the attacks the Act names.

03 PROVE

A readiness score, pass/fail by chapter, and the fixes.



Ascend AI EU AI Act assessment (illustrative)

SEE YOUR READINESS SCORE

Run Ascend AI against your own agents and chatbots for a chapter-by-chapter score.

RUN A READINESS ASSESSMENT

straiker.ai/eu-ai-assessment

ISO 27001 - SOC 2 TYPE II - SAAS, ON-PREM & SOVEREIGN-READY DEPLOYMENT

Source: Regulation (EU) 2024/1689, Official Journal, 12 July 2024. High-risk obligations apply in 2026 (Art. 113). Art. 99 penalties: up to EUR 15M or 3% of global turnover for high-risk non-compliance; EUR 35M / 7% applies only to prohibited practices under Art. 5.

This document maps Straiker capabilities to EU AI Act articles for information only and is not legal advice. Whether a system is high-risk, and which duties apply, depends on your use case and role. (c) 2026 Straiker Inc.