

Standard

NIST AI RMF

Governance relevance

Voluntary U.S. framework for AI risk management

ISO/IEC 42001

Certifiable AI management system

EU AI Act

Mandatory for high-risk AI in EU markets

OWASP Agentic Top 10

Agent-specific security vulnerabilities

Primary governance entry points

Govern and Measure functions most directly apply; full alignment spans all four pillars (Govern, Map, Measure, Manage)

Clause 8 (Operation) is the most relevant starting point; full certification requires mapping all clauses

High-risk requirements span Articles 9, 14, and related provisions; transparency obligations also apply to limited-risk systems including many agentic deployments

Ten agent-specific vulnerabilities require mapping across guardrail, access control, and monitoring components; review all ten, not only the most common three