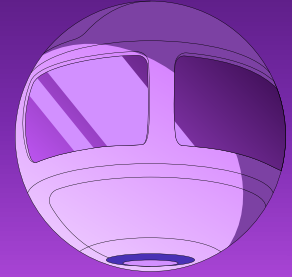


Cyera AI Security Readiness Assessment



The AI security landscape is evolving rapidly, creating an urgent need for organizations like yours to establish a robust security posture before risks materialize. The AI Security Readiness Assessment helps organizations determine how secure and mature their AI program truly is by establishing a detailed baseline of AI security maturity and developing a clear, actionable roadmap on how to move forward. The assessment enables organizations to:

Get the strategic foundation needed to deploy AI safely

Accelerate deployment of high-value AI use cases

Manage emerging risks across their entire AI ecosystem

Comprehensive security evaluation

Cyera experts will examine your AI program through a holistic lens, evaluating security and governance controls across the complete AI lifecycle. We'll focus on eight critical, and interconnected, domains that collectively determine your organization's ability to deploy AI safely and responsibly. And that no blind spots - from data models to operations - exist.

AI Governance	Policies, oversight structures, and responsible AI frameworks
Infrastructure	Network, compute, and cloud security for AI workloads
Interface Security	API, plugin, and integration security controls
Identity & Access	Authentication, authorization, and privilege management
Data Security	Training data protection, provenance, and privacy controls
Agent & Model Security	Development, deployment, and runtime protections
Application Security	Input validation, output filtering, and guardrails
Detection & Response	Monitoring, threat detection, and incident handling

What we review

The assessment produces quantifiable scores across four critical dimensions that determine true operational maturity, along with detailed evidence and specific recommendations.



Policy & Standards

Documented requirements, guidelines, and governance frameworks



Implementation

Technical capabilities and controls, processes, and tooling deployed in practice



Monitoring & Measurement

Visibility, metrics, testing, and compliance validation mechanisms



Improvement

Feedback loops, optimization programs, and proactive risk management

What you get

The assessment produces actionable deliverables designed to support immediate decision-making, drive AI security improvements, and enable ongoing program management. You will receive:

Executive brief that consists of a concise summary of top risks, critical decisions that need to be made, and business impact.

Gap analysis results across policy, implementation, monitoring, and improvement dimensions, a prioritized catalog of identified risks with severity ratings, potential impacts to the business, and recommended mitigations.

Maturity scorecard that provides an overall score, domain-specific ratings, and a visual outline of strengths and weaknesses.

Implementation roadmap that highlights 90-day quick wins and a twelve-month strategic initiatives outline.

For more information visit cyera.com or book a demo

Book a demo

