



Start Here

AI Security Maturity Assessment

Sylvan Assurance, LLC

2026-07-21

Contents

The one guide	1
The interactive assessment	1
When you outgrow the free tier	2

About This Document 3

Version 1 · Updated 2026-07-21

For anyone who wants to see where they stand with AI security before deciding whether to go further.

When you have worked through this, you will have: your free maturity result, and the five first fixes worth doing before anything else.

Your Free tier holds **1 document** (plus the interactive assessment). A “start here, in this order” guide only earns its place once there are several documents to sequence, so at this tier it is a single entry and a pointer onward.

The one guide

1. The First 5 AI Security Fixes

PDF · 20 min to read · Whoever has just been handed AI security

Five sequenced starter actions (take an inventory, read the training clause, write the never-paste rule, cut back access, decide the kill switch), with roughly a week allowed for each.

Reach for it when: First. It is the free starter, and the whole shape of the paid toolkit in miniature.

You finish with: Five named actions with dates against them.

The interactive assessment

Not a document: a short questionnaire that scores where you stand and points at the gaps.

→ Take the free AI security assessment.

When you outgrow the free tier

The Solo toolkit turns these five fixes into a worked programme (a written AI-tool register, a one-page acceptable-use policy, a first threat model, and more), with a real Start here catalog to sequence them.

→ See the Solo, Team and Enterprise editions.

About This Document

This document is part of the **AI Security Maturity Assessment**, produced by **Sylvan Assurance, LLC**.

It provides **general guidance and recommended practices** for securing systems that include AI and machine-learning components, drawn from widely recognised standards and frameworks (for example the National Institute of Standards and Technology (NIST) AI Risk Management Framework, International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) 42001, and the OWASP Top 10 for Large Language Model Applications). It is **not** a professional security audit, a penetration test, a certification, or legal advice, and it does not create any advisory or consulting relationship.

Every recommendation in this document is **optional** - a widely accepted way to reduce a common risk. You decide which recommendations to adopt, adapt, or decline. Following this guidance reduces exposure to common problems, but it **does not guarantee security and does not prevent any particular breach, incident, or loss**. Responsibility for the security of your business, systems, and data remains with you as the operator of your business.

Where this document refers to laws or regulations, it does so for general awareness only. Confirm your specific obligations with qualified legal counsel.

For full terms, see the Terms of Use provided with the AI Security Maturity Assessment.

Copyright 2026 Sylvan Assurance, LLC. Licensed for your own organisation's internal security use. Not for resale or redistribution.



Scan for the companion book to this toolkit.

sylvanassurance.com/go/ai-security

Sylvan Press · Sylvan Assurance, LLC · © 2026