Third-Party AI Risk Management

Vendor and third-party AI risk controls

Format	Duration	Audience	Deployment	LMS/SSO	PO
On-demand or facilitated	Scoped runtime	Risk, legal, procurement	Enterprise licensing	Optional	Supported

Executive Overview

Third-Party AI Risk Management is a structured program that helps organizations identify, assess, and control AI risk embedded in third-party products and services. It addresses due diligence, contracting considerations, and ongoing monitoring expectations for vendor-provided AI capabilities. The program is designed to support documented oversight, internal control alignment, and audit review through practical templates, governance-oriented guidance, and defensible review artifacts.

Program Outcome

Assess and manage third-party AI risk with defensible due diligence and controls.

Why This Matters

Organizations cannot rely on vendor assurances alone when AI capabilities are embedded in third-party products and services. A structured approach to due diligence, contracting, and ongoing monitoring helps reduce hidden exposure, strengthen accountability, and show that third-party AI risk has been handled in a documented, reviewable way.

Enterprise Risk Exposure Addressed

- Unvetted vendor AI use affecting enterprise data
- Opaque model behavior or change without notice
- Insufficient contractual protections and audit rights
- No ongoing monitoring of third-party AI controls

What the Organization Receives

- **Third-Party AI Due Diligence Questionnaire**: Data, model, security, and governance questions for vendors.
- **Contract & Control Guidance**: Control expectations, audit rights, change notification clauses, and contracting considerations.
- **Ongoing Monitoring Plan**: Review cadence, evidence requests, and issue tracking.
- **Risk Acceptance Template**: How to document exceptions and residual risk decisions.
- **Templates and Workbook Support**: Practical materials that reinforce consistent third-party AI oversight and governance alignment.