HARPONIAN
INTERNATIONAL

Third-Party & Vendor AI Risk

Governance Beyond Your Own Systems

Format	Duration	Audience	Deployment	LMS / SSO	PO
Live / Recorded	60 min	Board / Legal / Procurement	Enterprise licensing	N/A	Supported

Executive Overview

Third-Party & Vendor AI Risk is a live or recorded executive briefing that explains how AI risk enters the organization through vendors, platforms, service providers, and partners. It focuses on accountability, contract expectations, procurement controls, and the oversight questions leaders should ask beyond internal systems.

Briefing Outcome

Help executives, board members, legal, and procurement leaders understand vendor-introduced AI risk, clarify accountability boundaries, and strengthen oversight of third-party AI use.

Why This Matters

Organizations may face AI-related exposure even when they do not build or operate the AI system themselves. Vendors can introduce data, security, compliance, bias, transparency, and contractual risks that still affect the organization's customers, operations, and reputation.

Enterprise Risk Exposure Addressed

- Hidden AI functionality in third-party products or services
- Unclear accountability when vendor AI creates errors, exposure, or compliance concerns
- Contracts that do not address AI use, data handling, records, or audit rights
- Procurement reviews that miss AI-specific risk before adoption

What the Organization Receives

- **Vendor AI Risk Briefing:** Executive-level discussion of how third-party AI use creates governance and accountability exposure.
- **Vendor Question Set:** Practical questions for procurement, legal, security, and business owners to ask vendors.
- **Contract Control Notes:** Guidance on AI-related terms, data handling expectations, audit rights, and disclosure obligations.
- **Accountability Boundary Map:** Support for clarifying what the vendor owns, what the organization owns, and where shared responsibility exists.
- **Procurement Review Checklist:** Checklist for identifying AI functionality, sensitive data use, monitoring needs, and escalation triggers.