



Suhas Bhairav

AI Third-Party Security Review Guide

**A practical guide for IT leaders evaluating AI
vendor security**

A practical, repeatable framework to assess AI
vendors and safeguard data.

Suhas Bhairav

suhasbhairav.com

Scope & Criteria

AI vendor reviews must cover data access, hosting, identity controls, encryption, incident processes, certifications, subprocessors, and contract safeguards. This guide uses a risk-based, repeatable approach suitable for busy executives.

Key move Establish a formal vendor risk ownership with a named executive sponsor.

PRACTICAL CHECKLIST

- 01** Data access and least privilege: enforce minimal access and regular reviews.
- 02** Hosting and data residency: verify data location, separation, and provider controls.
- 03** Identity controls: require SSO, MFA; audit access logs.
- 04** Encryption: ensure at-rest and in-transit encryption and key management.
- 05** Incident response: defined breach notification timelines and contact points.
- 06** Certifications and audits: SOC 2, ISO 27001; request latest reports.
- 07** Subprocessors and data flow: maintain up-to-date list; assess cross-border transfers.

Suhas Bhairav AI Resource

A practical, repeatable framework to assess AI vendors and safeguard data.

Automated Review Process

Turn the vendor review into a repeatable process using checklists, scoring, and secure document intake. This page outlines practical steps to automate while preserving human oversight.

Key move **Guardrail: never auto-share sensitive data without audit trails.**

PRACTICAL CHECKLIST

- 01** Create a master inventory of AI vendors and data flows.
- 02** Use a standardized questionnaire covering access, hosting, encryption, incidents, and contracts.
- 03** Apply a 0-5 risk scoring rubric per category.
- 04** Automate document intake with a secure portal and AI extraction.
- 05** Set thresholds for automated actions; escalate high-risk items for human review.
- 06** Schedule quarterly reassessments; maintain evidence, owners, and risk posture logs.
- 07** Data/tools required: risk management system, secure portal, attestations, encryption details,

Suhas Bhairav AI Resource

A practical, repeatable framework to assess AI vendors and safeguard data.

Measurement, Ownership, and Guardrails

Establish governance to measure progress, enforce guardrails, and assign clear ownership. Define KPIs, approvals, and escalation paths.

Key move Ensure every high-risk decision has executive sign-off.

PRACTICAL CHECKLIST

- 01** Assign a vendor risk owner per domain to oversee reviews.
- 02** Define KPIs: vendors assessed, remediation time, and policy compliance rate.
- 03** Require formal approvals for high-risk findings and remediation plans.
- 04** Maintain auditable artifacts: reports, attestations, and decision logs.
- 05** Guardrails: prevent automated sharing of sensitive data without review.
- 06** Quarterly governance reviews to adjust risk appetite and controls.
- 07** Training: run monthly sessions on supplier risk management basics.

Suhas Bhairav AI Resource

A practical, repeatable framework to assess AI vendors and safeguard data.

ABOUT THE CREATOR

Suhas Bhairav

I build AI systems that combine distributed architecture, retrieval, knowledge graphs, security, and practical workflow design. My focus is AI that can be used repeatedly by real teams: understandable, reliable, and grounded in the work people already do.

EXPERTISE

- Principal systems architecture and applied AI engineering
- Production-grade AI systems, agentic workflows, RAG, and knowledge graphs
- Full-stack workflow applications across AWS, Google Cloud, Azure, on-premise, and hybrid environments
- Practical AI implementation patterns for automotive, manufacturing, finance, logistics, cybersecurity, sales, and customer operations
- Security, governance, observability, approvals, and failure-mode thinking for operational AI systems

WEBSITE

suhasbhairav.com

EMAIL

suhasbhairav@gmail.com