



Suhas Bhairav

AI Product Risk Review Kit

**Practical guardrails for usable, secure, and
compliant AI products.**

Deliver a repeatable, auditable risk review framework
before launch.

Suhas Bhairav

suhasbhairav.com

Usability, Reliability & User Experience

Assess how the AI feature will be used by customers and how reliably it performs. Define acceptance criteria and automation opportunities.

Key move **Action: establish a weekly usability sign-off by product and UX leads.**

PRACTICAL CHECKLIST

- 01** Define core user tasks the AI must complete and test against real, representative user stories.
- 02** Set measurable UX goals: completion rate, time-to-answer, error rates, and user satisfaction.
- 03** Automate basic usability checks (response length, clarity, tone) where possible.
- 04** Flag content or actions that require human review before user exposure.
- 05** Run reliability tests with diverse inputs and monitor latency under load.
- 06** Define fallback behaviors and graceful degradation for failures.
- 07** Document ownership: product manager owns UX review; engineering owns reliability gates.

Suhas Bhairav AI Resource

Deliver a repeatable, auditable risk review framework before launch.

Privacy, Security & Data Handling

Evaluate data flows, storage, and access controls for the AI feature. Align with privacy laws and internal policies.

Key move **Action: confirm data retention and deletion policy with legal.**

PRACTICAL CHECKLIST

- 01** Map data inputs, processing, and outputs; identify PII or sensitive information.
- 02** Set data minimization rules: collect only what is necessary.
- 03** Automate privacy checks: data retention, anonymization, and consent capture.
- 04** Enforce access controls and audit trails for all AI components.
- 05** Assess third-party model risks: vendor data handling and incident response.
- 06** Plan for data deletion and customer data requests.
- 07** Guardrails: cannot store or reuse outputs to infer sensitive data.

Suhas Bhairav AI Resource

Deliver a repeatable, auditable risk review framework before launch.

Safety, Misuse & Reputational Risk

Define safeguards to prevent harmful use, bias, and false claims. Establish monitoring and response protocols.

Key move Action: run a quarterly misuse risk tabletop with stakeholders.

PRACTICAL CHECKLIST

- 01** Define prohibited use cases and edge cases; implement user intent detection.
- 02** Implement misuse detectors and content filters; require human review for high-risk prompts.
- 03** Monitor for model hallucinations and provide confidence scores.
- 04** Add prompt-tacing and logging to trace decision rationales.
- 05** Prepare crisis protocol: incident response and external communications plan.
- 06** Assess reputational risk: potential biases and public perception.
- 07** Define ownership: security lead partners with product for risk gates.

Suhas Bhairav AI Resource

Deliver a repeatable, auditable risk review framework before launch.

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