Suhas Bhairav

AI Secure AI Deployment Checklist

Beginner-friendly, practical checklist for IT and security leaders.

A practical, step-by-step framework to deploy secure AI with guardrails.

Suhas Bhairav

suhasbhairav.com

Scope and Guardrails

Define the scope and guardrails for AI deployment in IT and security. This page outlines what to automate, what to review, and the data/tools needed.

Key move **Action: define and enforce least-privilege access before any AI deployment.**

PRACTICAL CHECKLIST

01	Automate provisioning of AI model access via IAM roles; require least privilege.
02	Week 1: automate data ingestion with access controls; mask sensitive fields.
03	Week 2: review prompts for sensitive data leakage; require human sign-off.
04	Map data flows: source → AI service → output; maintain data lineage.
05	Week 3: implement secrets vault and rotate keys.
06	Week 4: define tool permissions; grant only necessary APIs and features per role.
07	Logging: standardize event types, retention, and secure log transport.

Suhas Bhairav AI Resource

A practical, step-by-step framework to deploy secure AI with guardrails.

Data Flows, Access & Prompts

This page maps data flows, access controls, and prompt handling. It highlights what to automate and what to review.

Key move **Action: freeze production prompts until review process is in place.**

PRACTICAL CHECKLIST

01	Week 5: implement prompt injection testing and red-team simulation.
02	Logging: maintain secure log transport and retention.
03	Week 6: rotate secrets and audit access reviews.
04	Finalize data lineage documentation and data flows diagrams.
05	Data masking policies for training data; apply to inputs and outputs.
06	Week 7: conduct role-based access reviews and automation.
07	Vendor risk assessment: confirm security posture and data handling with providers.

Suhas Bhairav AI Resource

A practical, step-by-step framework to deploy secure AI with guardrails.

Monitoring, Incident Response & Vendor Risk

This page covers ongoing monitoring, incident response, red-teaming, and vendor risk management for AI deployments. It provides adoption steps and ownership.

Key move **Action: finalize incident response ownership and run a tabletop.**

PRACTICAL CHECKLIST

01	Week 8: incident response tabletop; refine playbooks.
02	RACI governance: assign owners for AI, data, security operations.
03	Measure KPIs: false positives, latency, data exposure, and consent adherence.
04	Audit and renewal: review vendor contracts and data sharing annually.
05	Weekly adoption note: document learnings and update playbooks.

Suhas Bhairav AI Resource

A practical, step-by-step framework to deploy secure AI with guardrails.

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