Suhas Bhairav

AI Security Policy Review Kit

A practical kit to audit policy coverage against live IT security systems.

A practical, auditable framework to align security policies with current systems and workflows.

Suhas Bhairav

suhasbhairav.com

Policy Ownership & Scope

Define policy scope, owners, and alignment with current systems. Use a lightweight RACI to map accountability.

Key move **Start with one policy area and map owners end-to-end.**

PRACTICAL CHECKLIST

01	Identify policies to include: access control, data handling, encryption, incident response, and third-party risk.
02	Assign policy ownership with a named owner, reviewer, and enforceable approver.
03	Map current systems and data flows under each policy.
04	Document exceptions process and escalation paths.
05	Identify data sources to validate policy coverage: asset inventory, IAM, logs, configurations.
06	List automation opportunities: policy-as-code, repo checks, and audit dashboards.

Suhas Bhairav AI Resource

A practical, auditable framework to align security policies with current systems and workflows.

What to Automate vs Review

Differentiate automation-ready checks from decisions that require human judgment. Specify data inputs and toolchain at outset.

Key move **Prototype one automated check this week; document results and lessons learned.**

PRACTICAL CHECKLIST

01	Automate policy existence checks in the policy repository and policy-as-code linting.
02	Automate data collection: asset inventory, IAM roles, access logs, and exceptions.
03	Keep human review for risk judgments, policy intent, and override approvals.
04	Required data/tools: policy repository, identity data, SIEM, config scans, evidence templates.
05	IT example: auto-check critical servers have approved SSH key rotation; trigger weekly reports.
06	Security example: MFA enforcement for admin roles; collect evidence via IAM and access logs.

Suhas Bhairav AI Resource

A practical, auditable framework to align security policies with current systems and workflows.

Adoption, Guardrails, & Metrics

Define practical cadence for reviews, approvals, and ownership across IT and Security. Establish metrics to measure policy effectiveness and compliance.

Key move **Document ownership and review dates in the policy registry.**

PRACTICAL CHECKLIST

01	Adopt a weekly sprint plan: map scope, gather data, implement pilot automation, review results.
02	Risks: false positives, scope drift, data exposure, or unapproved changes.
03	Guardrails: require approvals for policy changes and maintain an auditable change log.
04	Evidence: store versioned policy artifacts, test results, and access logs in a central repository.
05	Data protection: minimize data, encrypt sensitive artifacts, and limit access to policy owners.
06	Roles: assign policy owner, system owner, and security champion per domain.

Suhas Bhairav AI Resource

A practical, auditable framework to align security policies with current systems and workflows.

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