



Suhas Bhairav

AI Audit Evidence Collection Playbook

**Structured, auditable, automated evidence
collection for IT and Security controls**

A practical, repeatable framework to request, organize, validate, label, approve, and retain audit evidence across IT and security controls.

Suhas Bhairav

suhasbhairav.com

Define Controls & Evidence Streams

Clarify which IT and security controls require evidence and who owns each control. Establish evidence sources and data retention boundaries.

Key move Confirm ownership in writing; avoid ambiguous accountability.

PRACTICAL CHECKLIST

- 01** Map controls to evidence types (AC, IAM, vulnerability, change, incident) and required artifacts.
- 02** Identify control owners and data custodians for timely responses.
- 03** Define evidence sources: logs, tickets, configs, scans, and reports.
- 04** Set minimum retention windows aligned with compliance requirements.
- 05** Create standardized evidence request templates per control family.
- 06** Define naming, labeling, and versioning conventions.

Suhas Bhairav AI Resource

A practical, repeatable framework to request, organize, validate, label, approve, and retain audit evidence across IT...

Automate Evidence Requests and Labeling

Outline what to automate with AI-enabled agents, what requires human review, and how to validate data. Establish a baseline for coverage and quality.

Key move Never rely on raw logs without integrity verification.

PRACTICAL CHECKLIST

- 01** Automate evidence requests from SIEM, ticketing, and config stores using standardized templates.
- 02** Auto-label artifacts by control, source, date, and retention category.
- 03** Use agentic workflows to assemble evidence bundles for audits.
- 04** Flag incomplete or inconsistent artifacts for human review.
- 05** Maintain a lightweight version history for each artifact.
- 06** Require cryptographic hash or tamper-evident seals for critical items.

Suhas Bhairav AI Resource

A practical, repeatable framework to request, organize, validate, label, approve, and retain audit evidence across IT...

Adoption, Approvals, and Measurements

Describe adoption steps in weekly increments and the governance model. Include metrics to track success, risk, and retention.

Key move Document decisions; record deviations and rationale.

PRACTICAL CHECKLIST

- 01** Week 1: pilot in a single control family with a single data source.
- 02** Week 2: expand to IAM and change-management evidence; add labeling rules.
- 03** Week 3: integrate with an audit framework and define approvals.
- 04** Define approvals: control owner signs evidence bundles before retention.
- 05** Set KPI: time-to-collection, completeness, accuracy, and retention compliance.
- 06** Implement guardrails: data minimization, access controls, and revocation procedures.
- 07** Assign workflow ownership to a governance lead and an automation steward.

Suhas Bhairav AI Resource

A practical, repeatable framework to request, organize, validate, label, approve, and retain audit evidence across IT...

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