

## **AI Audit Checklist**

*(Lifecycle Coverage: Design → Training → Deployment → Monitoring)*

---

### **General Information**

- **Organization:** \_\_\_\_\_
- **Auditee Department/Team:** \_\_\_\_\_
- **Audit Date:** \_\_\_\_\_
- **Audit Type:**  Internal  External  Surveillance  Certification
- **Lead Auditor:** \_\_\_\_\_
- **Audit Team:** \_\_\_\_\_

---

### **1. Design Phase**

<b>Audit Question</b>	<b>Yes/No/NA</b>	<b>Evidence/Notes</b>
Have AI system objectives been clearly defined and aligned with business needs?		
Are AI ethical principles (fairness, accountability, transparency, privacy) integrated into design requirements?		
Has a <b>risk assessment (ISO/IEC 23894)</b> been conducted for potential ethical, technical, and societal risks?		
Is there documentation of stakeholders and their roles (AI provider, customer, subject)?		
Have data requirements and data sources been validated for quality and representativeness?		

---

### **2. Training Phase**

Audit Question	Yes/No/NA	Evidence/Notes
Is the training dataset representative of the intended user population?		
Have <b>data quality measures</b> (completeness, accuracy, timeliness, consistency) been applied?		
Have privacy and data protection regulations (e.g., GDPR, ISO/IEC 27701) been respected?		
Is there documentation of model selection and training methodology?		
Were bias detection and mitigation processes conducted during training?		
Has model validation been performed using separate validation/testing datasets?		

### 3. Deployment Phase

Audit Question	Yes/No/NA	Evidence/Notes
Was a formal go/no-go decision process conducted before deployment?		
Has the AI system been tested in a real-world pilot environment prior to full deployment?		
Are safeguards in place for <b>human control of technology</b> (e.g., human-in-the-loop for high-risk decisions)?		
Have stakeholders been informed of the AI system's purpose, scope, and limitations?		
Are security mechanisms in place to protect against adversarial attacks, data poisoning, or unauthorized access?		

Does the system comply with applicable legal and regulatory frameworks in deployment context?

#### 4. Monitoring & Post-Deployment

Audit Question	Yes/No/NA	Evidence/Notes
Is there ongoing monitoring of AI system performance against expected outcomes?		
Are <b>drift detection mechanisms</b> (concept drift, data drift) in place?		
Is there a process for handling user complaints, appeals, and grievances?		
Are audit logs and traceability records maintained for decisions made by the AI system?		
Is there a documented plan for <b>periodic retraining and re-validation</b> of the AI model?		
Have environmental, ethical, and societal impacts been reviewed post-deployment?		
Is there a process for decommissioning or retiring the AI system safely when needed?		

#### 5. Corrective Actions

- **Findings (Nonconformities, Observations, Opportunities for Improvement):**

---



---

- **Corrective Action Plan Owner:** \_\_\_\_\_
- **Deadline for Implementation:** \_\_\_\_\_
- **Follow-up Audit Required?**  Yes  No

---



This checklist ensures **end-to-end auditing** of AI systems in alignment with **ISO/IEC AI lifecycle governance**.