AI Security Compliance Checklist

Use this checklist to build a strong, secure, and compliant AI foundation—guided by trusted industry frameworks like **NIST AI RMF, ISO 42001, OWASP AI Model (AIMA), and the EU AI Act.**

Governance & Accountability

NIST • ISO • EU Act

Establish leadership, roles, and oversight for AI security and compliance.

- ◯ Define AI Roles & Owners for risk management and oversight.
- ◯ Develop AI Use & Security Policy covering acceptable practices and data usage.
- ◯ Maintain Formal AI Risk Register and review quarterly with stakeholders.
- ◯ Generate AI Risk & Compliance Reports for executives and boards.
- ◯ Document Human Oversight Procedures for high-impact AI decisions.

AI Inventory & Risk Identification

NIST • ISO • EU Act • OWASP

Achieve full visibility into AI assets and proactively identify risks.

- ◯ Create & Maintain an AI Bill of Materials (AI-BOM) listing models, datasets, APIs, and agents.
- ◯ Assign Ownership & Sensitivity Labels to all AI components.
- ◯ Validate AI Data Sources for quality and provenance (training/inference).
- ◯ Conduct AI Threat Modeling to identify risks like prompt injection or data poisoning.
- ◯ Perform Pre-deployment AI Risk Assessments for each new model or agent.

Security & Technical Controls

NIST • ISO • EU Act • OWASP

Implement robust safeguards to secure models, data, and behavior.

- ◯ Implement Input/Output Validation to prevent prompt injection and data leakage.
- ◯ Establish a Continuous AI Red Teaming Program to test model resilience.
- ◯ Apply Access Control & Encryption to protect model assets and prompts.
- ◯ Integrate AI Risk Checks into SDLC, CI/CD, and pull request processes.
- ◯ Review Third-Party AI Components for license compliance and malicious behavior.

Transparency & Lifecycle Assurance

NIST • ISO • EU Act • OWASP

Ensure traceability, accountability, and explainability throughout the AI lifecycle.

- ◯ Enable AI Decision Logging and audit trails for training events and outputs.
- ◯ Quantify AI Weaknesses using a standardized scoring system (e.g., AIWE).
- ◯ Create & Maintain Model Cards detailing purpose, risks, and limitations for all major AI systems.
- ◯ Conduct Bias and Fairness Assessments for all production AI models.
- ◯ Establish AI Runtime Monitoring to detect drift, hallucination, or data leakage.

Continuous Improvement & Compliance Proof

NIST • ISO • EU Act

Operationalize audits, incident response, and continuous enhancement.

- ◯ Develop and Test an Incident Response Plan for AI-related security or ethical failures.
- ◯ Conduct Periodic Internal Audits of AI risk management and compliance controls.
- ◯ Track and Validate Corrective Actions from AI incidents or audit findings.
- ◯ Perform Ongoing Post-market Monitoring for performance, bias, and security drift.
- ◯ Publish Transparency & Governance Statements to demonstrate trustworthy AI.