OWASP TOP 10 FOR LLMS SECURITY IMPLEMENTATION CHECKLIST

The Open Worldwide Application Security Project (OWASP) Top 10 for LLMs is a comprehensive approach to securing large language models (LLMs) applications throughout their development, deployment, and operational lifecycles. This checklist provides a non-exhaustive foundational methodology to identify, mitigate, and monitor security risks associated with LLMs using best practices from OWASP.

1. Planning & Architecture Security	COMPLETE
Conduct LLM-specific threat modeling using STRIDE-GPT and MITRE ATLAS frameworks.	☐
Define critical security boundaries between LLM components and map attack surfaces.	☐
Establish comprehensive data privacy, compliance, and risk management strategy.	☐
Document security requirements for model selection and system integration.	☐

2. Data & Model Supply Chain Security	COMPLETE
Perform security assessments of model vendors, data providers, and third-party components.	☐
Implement AI/ML Bill of Materials (BOM) with digital signing and provenance verification.	☐
Validate training data integrity and establish secure model storage with access controls.	☐
Scan all dependencies for vulnerabilities and establish update/patch management.	☐

3. Development & Testing Controls	COMPLETE
Implement multi-layered defenses against prompt injection and data poisoning attacks.	☐
Create robust input validation and output filtering for all LLM interactions.	☐
Conduct specialized adversarial testing targeting LLM-specific vulnerabilities.	☐
Integrate security testing into CI/CD pipeline with a focus on vector/embedding security.	☐

LLM OWASP TOP 10 SECURITY IMPLEMENTATION CHECKLIST

4. Deployment & Runtime Protection	COMPLETE
Establish defense-in-depth with authentication, authorization, and least privilege access.	☐
Implement resource quotas, rate limiting, and technical guardrails for LLM operations.	☐
Configure network segmentation and end-to-end encryption for sensitive data.	☐
Deploy human-in-the-loop oversight mechanisms for high-risk LLM actions.	☐

5. Operational Security	COMPLETE
Monitor anomalous usage patterns, prompt injection attempts, and resource consumption.	☐
Implement comprehensive logging with special focus on LLM inputs, outputs, and actions.	☐
Establish LLM-specific incident response procedures with clear escalation paths.	☐
Conduct regular security assessments and penetration testing against live systems.	☐

6. Governance & Compliance	COMPLETE
Document clear AI usage policies with model capabilities, limitations, and boundaries.	☐
Implement security training for all stakeholders interacting with LLM systems.	☐
Establish formal review process for model updates, plugins, and significant changes.	☐
Create a continuous improvement framework for security controls and compliance.	☐

NEXT STEPS

Need help getting ahead of AI risks and compliance challenges?

Contact Echelon Risk + Cyber to schedule an AI Governance or defensive posture assessment.

We defend the basic human right to security and privacy.

ECHELON RISK + CYBER