SSDLC Training — Checklist

Secure Code Review Checklist

Four-phase security-focused review process

Phase 1: Preparation

- ■ Review the change description and linked requirements
- ■ Understand the security context (data sensitivity, trust boundaries)
- ■ Check if SAST/DAST results are available for this change
- ■ Identify high-risk areas (auth, crypto, input handling, data access)

Phase 2: Security Review

- ■ Input validation present for all external data
- ■ No SQL injection, XSS, or command injection vectors
- ■ Authentication and authorization correctly enforced
- ■ Cryptographic operations use approved algorithms
- ■ Sensitive data not logged or exposed in error messages
- ■ No hardcoded secrets, tokens, or credentials

Phase 3: AI-Specific Review

- ■ AI-generated code identified and flagged for extra scrutiny
- ■ Hallucinated API calls or non-existent methods detected
- ■ AI code follows project coding standards (not just default AI style)
- ■ License compatibility verified for AI-suggested code patterns

Phase 4: Sign-Off

- ■ All security findings addressed or tracked as exceptions
- ■ SAST scan clean or findings triaged
- ■ Code review approved by qualified reviewer
- ■ Changes documented and linked to requirements