ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

Phase 1: Design & Planning

- [ ] **Threat modeling completed for new feature/product**

  Identify potential attack vectors, trust boundaries, sensitive data flows, and abuse scenarios before development begins.

- [ ] **Potential attack vectors documented**

  Document how attackers could misuse APIs, user interfaces, third-party integrations, or privileged access points.

- [ ] **Trust boundaries identified**

  Define where data moves between systems, services, users, and external parties to understand security exposure.

- [ ] **Security risks prioritized and assigned owners**

  Classify risks by severity and ensure each risk has a responsible owner for mitigation.

- [ ] **Approved development tools defined**

  Maintain a list of approved development, CI/CD, AI, and collaboration tools that meet company security requirements.

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

- [ ] **AI coding assistants evaluated and approved**

  Review AI tools for data privacy, code ownership, compliance, and security risks before adoption.

- [ ] **Data privacy requirements documented**

  Define how sensitive, customer, and regulated data must be collected, stored, processed, and retained.

- [ ] **Authentication requirements defined**

  Specify authentication mechanisms such as SSO, MFA, OAuth, or password standards.

- [ ] **Authorization requirements documented**

  Clearly define user roles, access rights, and privilege boundaries.

- [ ] **Encryption standards specified**

  Establish approved encryption methods for data in transit and at rest.

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

Phase 2: Development

- [ ] **Developers trained on secure coding standards**

  Ensure engineering teams understand secure coding practices and common vulnerability patterns.

- [ ] **OWASP Top 10 risks reviewed**

  Validate that teams understand the most common web application security risks and mitigation strategies.

- [ ] **Mandatory peer review enforced**

  Require independent review before any code is merged into production branches.

- [ ] **AI-generated code reviewed by humans**

  Verify that engineers review AI-assisted code for security issues, logic errors, and compliance risks.

- [ ] **SCA tool integrated into CI pipeline**

  Automatically scan third-party dependencies for known vulnerabilities.

- [ ] **Vulnerable dependencies monitored**

  Continuously track security updates and vulnerability disclosures affecting software dependencies.

- [ ] **Critical dependency updates prioritized**

  Define SLAs for updating high-risk libraries and frameworks.

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

Phase 3: Testing & Verification

- [ ] **SAST integrated into CI pipeline**

  Automatically analyze source code and detect vulnerabilities before deployment.

- [ ] **DAST implemented on test environments**

  Continuously test running applications for exploitable vulnerabilities.

- [ ] **Security scans included in release process**

  Make security validation a mandatory release requirement.

- [ ] **High-severity findings block deployment**

  Prevent production releases when critical vulnerabilities remain unresolved.

- [ ] **Penetration testing completed for critical systems**

  Simulate real-world attacks against high-risk applications and services.

- [ ] **Authentication mechanisms tested**

  Validate login flows, MFA controls, session management, and password policies.

- [ ] **Authorization logic validated**

  Ensure users cannot access resources or actions beyond their authorized permissions.

- [ ] **Security sign-off obtained**

  Require formal approval from security stakeholders before release.

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

Phase 4: Deployment & Operations

- [ ] **Pipeline access restricted**

  Limit CI/CD access to authorized personnel using least-privilege principles.

- [ ] **Secrets managed securely**

  Store credentials, keys, and tokens in approved secrets management platforms.

- [ ] **Build artifacts validated**

  Verify integrity, authenticity, and traceability of deployment packages.

- [ ] **MFA enforced for production access**

  Require multi-factor authentication for all privileged access to production systems.

- [ ] **Least-privilege model implemented**

  Grant only the minimum permissions required to perform a business function.

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

- [ ] **Infrastructure hardening completed**

  Disable unnecessary services, close unused ports, and apply secure configurations.

- [ ] **Security logging enabled**

  Capture security-relevant events across applications, infrastructure, and identity systems.

- [ ] **Critical events monitored**

  Establish alerting and monitoring for suspicious activities and security incidents.

- [ ] **Incident response contacts documented**

  Maintain an up-to-date escalation path and incident response ownership model.

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

Final Validation Before Release

- [ ] **No critical vulnerabilities remain**

  Verify all critical findings have been remediated or formally accepted through risk governance.

- [ ] **Security review completed**

  Conduct a final security assessment of architecture, code, infrastructure, and configurations.

- [ ] **Penetration testing approved**

  Confirm results have been reviewed and remediation activities completed.

- [ ] **Monitoring operational**

  Ensure logs, alerts, dashboards, and response workflows are functioning correctly.

- [ ] **Rollback plan documented**

  Define how to safely revert releases if operational or security issues occur.

- [ ] **Business owner approval received**

  Verify business stakeholders accept operational and residual security risks.

- [ ] **Security owner approval received**

ekino.

Secure SDLC Checklist

Design → Deployment Security Review Framework

For: CTOs, Engineering Managers, Security Leads

Goal: Validate that security controls are embedded throughout the SDLC

Quick Assessment

Scoring

Status	Score
Completed	1
Not Completed	0

Total Score: ___ / 48

Result	Security Readiness
0 - 24	High Risk
25 - 36	Foundational
37 - 44	Managed
45 - 48	Mature