

Secure software delivery

A release-readiness conversation for engineering and security teams.

Choose one application and its next release. Mark each item Ready, Partial, or Unknown. Record the evidence and the person who can resolve each open question.

01 / Define the release boundaries

Identify the application owner, sensitive data, exposed interfaces, and security requirements. Keep a short threat review with the release record.

02 / Protect code and credentials

Use reviewed changes and appropriate repository access. Keep secrets out of source code and build logs; document rotation and access ownership.

03 / Know what you ship

Inventory dependencies and build inputs. Review vulnerability findings, artifact integrity, and documented risk decisions before release.

04 / Make security checks actionable

Use appropriate code, dependency, and application tests in the delivery process. Agree which findings block a release and who can approve an exception.

05 / Prepare deployment and rollback

Separate environments, limit deployment permissions, and document rollback steps. Test those steps and retain the release evidence.

06 / Plan for vulnerabilities after launch

Name a vulnerability intake owner and response process. Track remediation, communicate with affected stakeholders, and review recurring root causes.

YOUR NEXT STEP

Take the most consequential unresolved item into release planning. Agree a decision owner and acceptance criteria before adding another tool or pipeline check.

Open release decision: _____ Owner: _____ Due: _____

Reference: NIST Secure Software Development Framework

Educational checklist informed by the NIST SSDF. Tailor it to your application; it does not establish compliance or guarantee a secure release.