CNCF Project Release Guidelines

Version History

Date	Version	Author(s)	Changes
2025-08-21	0.1	Matt Young	Initial draft, Created formal Initiative from this version: https://github.com/cncf/toc/issues/1849

Reviewers

Date	Name	Contact

Initiative: CNCF Project Release Guidelines

Create guidelines, patterns, and reference implementations to help CNCF projects establish robust, secure, and repeatable release workflows.

Responsible group: TAG Operational Resilience
Primary contact: Jeremy Rickard
Additional contacts: Leadership from TAG Security and TAG Operational Resilience.

Description

This initiative will create a comprehensive set of guidelines, patterns, and reference implementations to help CNCF projects establish robust, secure, and repeatable release workflows. This provides a practical framework for projects to align with the CNCF's obligations under regulations like the EU's Cyber Resiliency Act (CRA).

The need for this guidance was first proposed by Karena Angell during the public TOC meeting on August 19th, 2025, in response to recurring needs identified during project due diligence. The outcome will be a valuable toolkit that empowers project maintainers to enhance security, improve transparency, and deliver software to their communities with greater confidence and predictability.

Related Initiatives

- [Initiative]: CNCF Software Supply Chain Insights · Issue #1709
- [Initiative]: CNCF Project Capabilities Badging Framework · Issue #1711
- (forthcoming) TAG Security Initiative that will provide relevant guidance on SBOM generation, signing, and other security artifacts (TODO link once created)

Scope and Goals

The scope of this initiative is to research and document guidelines covering the following topics:

- **Versioning and Branching:** Establish clear recommendations for versioning schemes (e.g., Semantic Versioning) and sustainable git branching strategies for release management (e.g., release branches, hotfixes).
- **Release Planning and Cadence:** Provide patterns for transparent release planning, public roadmapping, and establishing a predictable release cadence that is appropriate for the project and that builds Adopter trust.
- **Changelogs and Release Notes:** Document good practices for maintaining clear, human-readable changelogs and generating informative release notes, including the use of automation via standards like Conventional Commits.

- **Automation and Tooling:** Identify and provide reference examples for tooling and CI/CD pipelines (e.g., GitHub Actions, GoReleaser) to create automated, repeatable, and reliable release workflows.
- **Security Artifact Integration:** This initiative will coordinate with TAG Security to consume the deliverables from a **to-be-created, dedicated initiative within TAG Security**. That initiative will provide the formal guidance on the generation, signing, and distribution of essential security artifacts (e.g., SBOMs, VEX documents, SLSA attestations, and digital signatures), which will be integrated as a standard part of these release guidelines.

Non-Goals

- This initiative will **not** mandate a specific release cadence or frequency for projects.
- It will **not** enforce the use of any single, specific tool, instead offering a range of well-documented options.
- It will **not** create a strict, pass/fail compliance regime; the goal is to provide a clear framework and path to improvement, not to create a barrier.

Deliverable(s) or exit criteria

The initiative will produce a multi-faceted set of deliverables designed for practical adoption:

- A **published guide** on the CNCF website covering the patterns and practices for all topics defined in the Goals section.
- A collection of **templates and reference implementations** that projects can directly adopt or adapt to streamline their release workflows. Examples include reusable GitHub Actions and Checklists.
- A **proposal for a Rubric** that can be used by the [Initiative]: CNCF Project Capabilities Badging Framework · Issue #1711 for potential future "Release Practices" badge(s).

The initiative will be considered complete when these three deliverables are published and handed off to the relevant groups for maintenance.