Releasing a third-party library

The release of a new third-party library, top to bottom. The first five points end the check on the spot, the soft criteria below only feed the verdict.

Hard, any one point ends the check

- [ ] **Licence**
  Forbidden or unknown counts as a finding. A licence you cannot establish is not a release.
- [ ] **Name**
  On the blocklist or suspiciously close to a known package name: it stops here.
- [ ] **Known vulnerability**
  The checked version carries an unpatched flaw of high severity.
- [ ] **Source**
  There is no public source repository. What nobody can read, nobody checks.
- [ ] **Age**
  The package is younger than 90 days.

Soft, every point feeds the verdict

- [ ] **Who writes it**
  If nine in ten commits come from one person, the project is orphaned the day that person leaves.
- [ ] **Last commit**
  For a living project we expect activity within the last week. For a finished library three to four months is fine. Years never.
- [ ] **Open reports**
  Old feature requests may sit. Real defects older than a year are a warning sign.
- [ ] **Who carries it**
  A foundation behind it counts. Work under company accounts counts. Inclusion in the vetted part of a major distribution counts.

Before it goes in

- [ ] **Waiting period**
  New versions arrive 14 days late, on purpose. In two analysed attacks on package registries the poisoned versions were available for hours only.
- [ ] **Record**
  Every fetched value goes into a file in the repository with the time it was fetched. After that the build asks nothing, it only compares.
- [ ] **Outcome**
  Accept, reject, signed exception, or fork and maintain it yourself. A rejection you forget becomes an acceptance next time.

A signed exception with a reason and a name lifts any of these findings. One it does not: the blocklist.