Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Cancelleria federale CaF

Trasformazione digitale e governance delle TIC TDT

14.09.2026

Em002-2.2 Lista di controllo Analisi e preparazione OSS

Versione 2.0-5b1a0ad

Indice

La presente lista di controllo fa parte del documento *Em002-2 Istruzioni per la pubblicazione di software open source* ed è destinata agli specialisti TIC.
Serve a esaminare la documentazione e il codice sorgente di un progetto. Contribuisce così a garantire che il livello qualitativo della documentazione sia sufficiente per pubblicare un'applicazione come open source. Consente inoltre di verificare che il codice sorgente e tutti i componenti di terzi utilizzati dal progetto non comportino rischi giuridici. Queste misure riducono al minimo i rischi per la sicurezza.
Le informazioni su questa lista di controllo figurano in *[Em002-2]*, capitolo 4.

Questa lista di controllo garantisce inoltre che la documentazione di progetto si rivolga in egual misura agli utenti finali e agli specialisti tecnici.

1. Oggetto

1.1. Nome e breve descrizione del software

Indicate il nome del software.

1.2. Persona di contatto ed esame

Indicate l'organizzazione, la persona di contatto del servizio specializzato nonché le persone responsabili (p. es. ISBO/DSBO) che hanno verificato il rispetto delle prescrizioni di pubblicazione.

2. Lista di controllo

	☐ La *lista di controllo Em002-2.1 Valutazione preliminare OSS* è stata compilata e non sono stati rilevati punti problematici.

☐ Il codice sorgente da pubblicare è stato analizzato.

Verificare come sono state attuate la qualità del codice esistente e le direttive.

Assicurarsi che non siano contenuti dati (di test) sensibili, p. es. dati basati su persone o casi reali.

Documentazione aggiornata (cfr. [Em002-2] allegati D.1. e D.2.)

Cancellare i file superflui o i documenti obsoleti.

Verificare il codice alla ricerca di segreti o credenziali.[1]

Svolgere test di sicurezza mirati e istituire in seguito un programma di bug bounty (pubblico).[2]

Esaminare tutte le librerie utilizzate per accertare che le licenze siano disponibili e che siano stati redatti i relativi elenchi (attribuzioni).

Descrizione del deployment (pipeline CI/CD[3]) ed eventualmente allestimento di un'istanza dimostrativa.

☐ Scelta della licenza

Verificare eventuali dipendenze da licenze esistenti.

Per il codice di terzi, verificare la compatibilità delle condizioni d'uso con la licenza prevista e, se necessario, sostituire il codice.

Scegliere la licenza adeguata sulla base della guida «Em002-3 Guida alle licenze OSS» (le raccomandazioni principali sono l'AGPL per il copyleft e la MIT per le licenze permissive).

Licenza scelta e motivazione

☐ La documentazione è archiviata insieme al codice sorgente (cfr. [Em002-2] allegato D.1.)

Motivazione / luogo di archiviazione

☐ La documentazione si rivolge sia agli utenti finali sia agli specialisti tecnici.

Elenco della documentazione centrale

☐ Documentazione dettagliata del codice sorgente (specifica per l'OSS)

La documentazione standard importante (README, LICENSE, CONTRIBUTING ecc.) è disponibile.

1. https://www.ncsc.admin.ch/ncsc/it/home/aktuell/im-fokus/2022/git.html
2. https://www.ncsc.admin.ch/ncsc/it/home/infos-fuer/infos-it-spezialisten/themen/bug-bounty-programme.html
3. https://it.wikipedia.org/wiki/CI/CD

	☐ Il codice sorgente, cronologia compresa, non contiene dati personali sensibili, protetti o confidenziali. Oppure la cronologia è stata cancellata completamente. (cfr. [Em002-2] allegato E.2.) Spiegazione dell'esame (se non archiviata come documento separato)
	☐ Con il fornitore e con tutti gli sviluppatori coinvolti in seno all'Amministrazione federale è stato chiarito se le indicazioni sugli autori (nomi, indirizzi e-mail) possono essere pubblicate. In alternativa il codice sorgente, cronologia compresa, è stato ripulito o anonimizzato.
	☐ Le librerie utilizzate dal progetto sono compatibili con la licenza del progetto. Spiegazione dell'esame (se non archiviata come documento separato)
	☐ Il progetto utilizza un gestore di pacchetti per gestire le proprie dipendenze.
	☐ Il progetto dichiara la propria licenza nel corrispondente descrittore del gestore di pacchetti. Allestimento di una Software Bill of Materials (SBOM) che elenca tutti i componenti open source utilizzati.
	☐ Il codice sorgente contiene un file *THIRD-PARTY-LICENSES.md* che indica per ogni libreria utilizzata: il nome del progetto della libreria, la sua homepage, l'identificatore SPDX della sua licenza e un collegamento alla stessa.
	☐ Per le applicazioni è disponibile una finestra di dialogo «Informazioni su» che rinvia al file *THIRD-PARTY-LICENSES.md*.
	☐ Nell'ambito del processo di code review si garantisce che il file *THIRD-PARTY-LICENSES.md* venga aggiornato a ogni modifica delle librerie.

3. Osservazioni conclusive

Osservazioni e rinvii ad altri documenti rilevanti

Archiviazione del modulo

Archiviate questo modulo insieme alla documentazione di progetto e/o conformemente alle prescrizioni della vostra autorità (unità organizzativa).